

公告本

379308

申請日期	87 年 4 月 15 日
案 號	87105738
類 別	G09C 1/0

A4
C4

379308

(以上各欄由本局填註)

發 明 專 利 說 明 書		
一、發明 名稱	中 文	密碼化裝置及方法、解碼裝置及方法、以及資訊處理裝置及方法
	英 文	
二、發明 創作人	姓 名	(1) 石黑隆二 (2) 大澤義知 (3) 刑部義雄
	國 籍	(1) 日本 (2) 日本 (3) 日本
		(1) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社
	住、居所	(2) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社 (3) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社
三、申請人	姓 名 (名稱)	(1) 蘇妮股份有限公司 ソニー株式会社
	國 籍	(1) 日本
	住、居所 (事務所)	(1) 日本國東京都品川區北品川六丁目七番三五號
	代 表 人 名 姓	(1) 出井伸之

裝

訂

線

379308

申請日期	87 年 4 月 15 日
案 號	87105738
類 別	

A4

C4

(以上各欄由本局填註)

發 明 專 利 說 明 書		
一、發明 名稱	中 文	
	英 文	
二、發明 人	姓 名	(4) 佐藤真 (5) 嶋久登 (6) 淺野智之
	國 籍	(4) 日本 (5) 日本 (6) 日本 (4) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社
	住、居所	(5) 美國加州帕索佛拉斯賽拉托格、美國研究實驗室 US Reserch Laboratories 12610 Paseo Flores Saratoga, CA 95070 U.S.A (6) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社
三、申請人	姓 名 (名稱)	
	國 籍	
	住、居所 (事務所)	
	代 表 人 姓 名	

裝

訂

線

(由本局填寫)

承辦人代碼：
大 類：
I P C分類：

A6
B6

本案已向：

國(地區) 申請專利，申請日期： 案號： ，☐有 ☐無主張優先權

日本 1997 年 4 月 23 日 9-106136 ☒有主張優先權

有關微生物已寄存於： ，寄存日期： ，寄存號碼：

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

經濟部中央標準局員工消費合作社印製

四、中文發明摘要(發明之名稱：密碼化裝置及方法、解碼裝置及方法、以及資訊處理裝置及方法)

本發明的課題係為確實地防止不當的複製。

其解決手段：以DVD播放機1的1394介面26所被暗碼化之資料，經由1394匯流排，傳輸到個人電腦2及磁光碟裝置3。在於變更功能未開放給使用者之磁光碟裝置3，以1394介面36的解碼所收訊的資料。對於此點，在於變更功能已開放給使用者之個人電腦2，以1394介面49，用時變鍵i解碼暗碼化的資料，在應用部61用時段鍵S進而解碼其解碼其解碼結果。

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

英文發明摘要(發明之名稱：)

五、發明說明(1)

〔發明所屬領域〕

本發明係為關於密碼化裝置及方法，解碼裝置及方法，以及資訊處理裝置及方法；特別是關於使其更提高安全性之密碼化裝置及方法，解碼裝置及方法，及其資訊處理裝置及方法。

〔發明背景〕

將代表性電腦等之複數個電子機器，以匯流排相互連接，構成網路，而使其在網路內可以相互收授各種資料。

其結果，例如，以被連接在網路之D V D播放器，而可以將從D V D所再生的影像資料，介由匯流排，傳輸，顯示在電視顯視機，監視器等之顯示裝置。通常，將D V D所再生的影像顯示在顯示裝置而作視聽，係為在於購入D V D的時刻，著作權者所容許的情況。

不過，將D V D所再生的資料，複製在其他記錄媒體後使用，一般是不被著作權者所容許。因此，為了防止介由匯流排（網路）而送出之資料被不法複製，所以在於送出側，使資料密碼化；在於收訊側，解碼此資料已被考慮到。

不過，D V D播放器，電視顯像機等的消費性機器（C E機器），通常是為了所定的目的而被設計・製造；使使用者無法改造此狀況或組裝其他零件而取得裝置內部的資料且繕改（變更功能）下被製造。對於此點，例如個人電腦，大多數的情況，公開結構體系或電路；由於追加連

（請先閱讀背面之注意事項再填寫本頁）

訂

五、發明說明(2)

接埠，安裝各種的應用軟體，因而使其可以追加，變更種種的功能。

因此，在於個人電腦，將該內部匯流排上的資料，附加所定的硬體，作成軟體程式，可以較容易地直接查看，改繕個人電腦內部的匯流排上資料。此情況，例如以個人電腦取得在從DVD播放器密碼化而傳送至電視顯像機的資料，將此資料解碼後複製，係為意味著在作成應用軟體下，能容易進件。

換言之，個人電腦，希望是介由匯流排連接進行通訊的連結部，及準備收發訊的資料，利用所收訊的資料之應用部；物理上，邏輯上，在該處使用者可以使用之部分較多。對於此點，在於CE機器，兩者的連接為密接，幾乎沒有使用者可以介入的部分。

[發明所欲解決之課題]

本發明係為鑑於此狀況，使其更確實地防止資料的不法複製。

[實施形態]

第1圖係為表示適用本發明之資訊處理系統之構成例。在於該構成例，介由IEEE 1394系列匯流排11而相互連接DVD播放器1，個人電腦2，光磁碟裝置3，資料播放收訊裝置4，監視器5，電視顯像機6。

第2圖係及表示其中的DVD播放器1，個人電腦2

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明(3)

，及磁光碟裝置之內部的更詳細構成例。DVD播放器1係為介由1394介面26而被連接至1394匯流排11。CPU21係為根據被記憶在ROM22的程式而執行各種的處理；RAM係為在於CPU21執行各種的處理時適切記憶必要的資料或程式。操作部24，係為以按鍵，開關，遙控器等所構成，當使用者進行操作時，輸出對應於該操作的訊號。驅動器25，係為驅動DVD（光碟）（未圖示），使其再生被記錄在該處之資料。

EEPROM27係為在裝置的電源OFF後也能記憶所必要記憶的資訊（此實施形態的情況，鍵資訊）。內部匯流排28係為相互連接這些各部分。

磁光碟裝置3具有CPU31至內部匯流排38。具有與在上述過DVD播放器1之CPU21至內部匯流排28同樣的功能，其說明則省略。不過，驅動器35，係為驅動磁光碟（未圖示），在該光磁碟使其記錄或是再生資料。

個人電腦2係為介由1394介面49而被連接至1394匯流排11。CPU41係為根據被記憶在ROM42的程式而執行各種的處理。在RAM43，適切記憶著在於CPU41執行各種的處理所必要的資料或程式等。在輸入出介面44，被連接有鍵盤45及滑鼠46等。使其從這些裝置所輸入的訊號輸出至CPU41。另外，在輸入出介面44，被連接有硬碟（HDD）47，使其可以在該處記錄再生資料，程式等。在輸入出

（請先閱讀背面之注意事項再填寫本頁）

訂

五、發明說明(4)

介面 4 4 另外使其適切裝著擴充埠 4 8，可以附加必要的功能。在 E E P R O M 5 0 使其記憶在電源 O F F 後也能保持所必要的資訊（此實施形態的情況，各種的鍵入資訊）。例如，以 P C I（Peripheral Component Interconnect），區間匯流域所構成之內部匯流排 5 1，係為使其相互連接這些各部分。

然而，此內部匯流排 5 1 係為對使用者開放；使用者係為在擴充埠 4 8 適切連接所定的連接埠，作成所定的軟體程式後安裝，而使其適切收訊以內部匯流排 5 1 所被傳輸的資料。對於此點，在於 D V D 播放器 1 或磁光碟裝置 3 等的消費性電子（C E）裝置，內部匯流排 2 8 或內部匯流排 3 8，來被開放給使用者，只限於進行特殊的改造等，使其無法取得傳輸到該匯流排之資料。

其次，說明在所定的始源端與接收端之間所進行之鍵認處理。此鍵認的處理，係為如第 3 圖所示，在於作為始源端的例如作為預先被記憶在 D V D 播放器 1 的 R O M 2 2 之軟體程式的 1 種之固件 2 0，與作為接收端的例如被記憶在個人電腦 2 的 R O M 4 2，作為 C P U 4 1 所處理的軟體程式的 1 種之許可管理 6 2 之間被進行。

第 4 圖係為表示在於始源端（D V D 播放器 1）與接收端（個人電腦 2）之間所進行的鍵認順序。在 D V D 播放器 1 的 E E P R O M 2 7，預先被記憶有服務鍵（service_key）及函數（hash）。這些都是從著作權者，所

（請先閱讀背面之注意事項再填寫本頁）

訂

五、發明說明(5)

提供給此 DVD 播放器 1 的使用者；各使用者將此秘密的保管在 EEPROM 27。

服務鍵係為被加諸在著作權者所提供的每個資訊；在於以此 1394 匯流排 11 所構成之系統為共通的。然而，在於本說明書，系統係為表示以複數個裝置所構成之全體裝置。

hash 函數係為對於任意長的輸入，輸出 64 位元或是 128 位元的固定長資料；設為 $Y (= hash(x))$ 時，造成求出 x 會有困難，且求出成為 $hash(x_1) = hash(x_2)$ 之 x_1 及 x_2 的組合也會有困難之函數。作為 1 方向 hash 關數的代表性函數，已知有 MD5 或 SHA。關於此 1 方向 Hash 函數，在 Bruce Schneier 著的「Applied Cryptography (Second Edition), Wiley」已被詳細地解說。

另則，作為接收端之例如個人電腦 2，係為將從著作權等所供予個人所屬之固有識別編號 (ID) 及許可鍵 (license_key) 秘密的保持在 EEPROM 50。此許可鍵係為對於連結幾位元的 ID 及 n 位元的服務鍵所得到的 $n + m$ 位元之資料 ($ID || service_key$)，適用 hash 函數而得到之值。即是許可鍵以下式表示。

$$license_key = hash(ID || service_key)$$

作為 ID 例如可以使用 1394 匯流排 11 的規格所

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明(6)

訂定之 node_unique_ID。此 node_unique_ID，係為如第 5 圖所示，以 8 位元組（64 位元）所構成；最初的 3 位元組，係為以 I E E E 所管理，從 I E E E 提供給電子機器的各製造廠。另外，下位 5 位元組，係為各製造廠可以提供給使用者所使用的裝置。各製造廠，例如對於下位 5 位元組，在系列使其 1 台分配 1 個編號，使用了全部 5 位元組分時，上位 3 位元組進行接受提供形成為別的編號之 node_unique_ID，然而，針對該下位 5 位元組，使其 1 台分配 1 個編號。因此，此 node_unique_ID，不拘限於製造廠，每一台都是不同，在各裝置形成為固有的 I D。

在於步驟 S 1，DVD 播放器 1 的固件 20，係為控制 1394 介面 26，介由 1394 匯流排 11 而對於個人電腦 2 要求 I D。個人電腦 2 的許可管理 62，係為在於步驟 S 2，收訊此 I D 的要求。即是 1394 介面 49，係為介由 1394 匯流排 11 而收訊從 DVD 播放器 7 所傳輸到來的 I D 要求訊號，則將此訊號輸出至 CPU 41。CPU 41 的許可管理 62，係為接受此 I D 要求時，在於步驟 S 3，讀出被記憶在 EEPROM 50 的 I D，將此 I D 介由 1394 介面 49 而從 1394 匯流排 11 傳輸至 DVD 播放器。

在於 DVD 播放器，在步驟 S 4，1394 介面 26 接收此 I D，則此 I D 被供給到以 CPU 21 所動作的固件 20。

固件 20 係為在於步驟 S 5，結合從個人電腦 2 受理

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明(7)

傳輸之ID，及被記憶在EEPROM27之服務鍵，而生成資料(ID || serviec_key)，對於此資料，如次式所示適用Hash函數，生成鍵lk。

$$lk = \text{hash}(\text{ID} || \text{serviec_key})$$

其次，在於步驟S6，固件20係為生成密碼鍵sk。此密碼鍵sk之詳情於後述，但此密碼鍵sk係為在於DVD播放器1及個人電腦2分別被利用，作為時段鍵。

其次，在於步驟S7，係為以步驟S5所生成之鍵lk作為鍵，將步驟S6所生成之密碼鍵sk密碼化，而得到密碼化資料(密碼化鍵)e。即是運算下式。

$$e = \text{Enc}(lk, sk)$$

然而，Enc(A, B)係為意味著以共通鍵密碼方式，用鍵A，而將資料B密碼化。

其次，在步驟S8，固件20係為將步驟S7所生成之密碼化資料e傳輸到個人電腦2。即是此密碼化資料e，從DVD播放器1的1394介面26，介由1394匯流排11而被傳輸到個人電腦2。在於個人電腦2，在步驟S9，介由1394介面49而收訊此密碼化資料e。許可管理62，係為將經該過程所收訊的密碼化資料記憶在EEPROM50之許可鍵作為鍵，而如下述地解碼

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明(8)

，生成解碼鍵 sk' 。

$$sk' = \text{Dec}(\text{license_key}, e)$$

然而，此處， $\text{Dec}(A, B)$ 係為意味著以共通鍵密碼方式用鍵 A ，而解碼資料 B 。

然而，以此共通鍵密碼化方式之密碼化運算，已知有 DES。針對共通鍵密碼化方式也是在上述過之 Applied Cryptography (Second Edition) 已被詳細解過。

在於 DVD 播放器 1，在步驟 S5 所生成之鍵 lk 形成為與被記憶在個人電腦 2 的 EEPROM 50 (license_key) 同一之值。即是成立下式。

$$lk = \text{license_key}$$

因此，在於各個電腦 2，在步驟 S10 所解碼而得到之鍵 sk' ，係為在於 DVD 播放器 7，形成為與在步驟 S6 所生成之密碼鍵 sk 同一之值。即是成立下式。

$$sk' = sk$$

此樣，在於 DVD 播放器 1 (始源端) 及個人電腦 2 (接收端) 的兩者，可以共有同一的鍵 sk ， sk' 。在該處，將此鍵 sk 原樣作為密碼鍵所用，或是以此為根基

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明(9)

，分別作成疑似亂數，將此用作為密碼鍵。

許可鍵，係為由於是在各裝置根據對應於固有的 I D 及所提供的資訊之服務鍵而被生成，所以其他裝置無法生成 s k 或是 s k'。另外，著作權者所未認可之裝置，因未具有許可鍵，所以無法生成 s k 或 s k'。因此，其後 D V D 播放器 1 使用密碼鍵 s k，將再生資料密碼化後傳輸到個人電腦 2 時，當個人電腦 2 得到適切的許可鍵之情況，因具有密碼鍵 s k'，所以可以解碼由 D V D 播放器所傳輸到來的被密碼化再生資料。不過，個人電腦 2 未得到適切的許可鍵時，因未具有暗碼鍵 s k'，所以無法解碼傳輸到來所被密碼化之再生資料。換言之，因只有適切的裝置可以生成共通的暗碼鍵 s k，s k'，結果是形成為進行鑑認。

如果 1 台個人電腦 2 的許可鍵被盜用，因 I D 為每台相異，所以用該許可鍵，其他裝置無法解碼從 D V D 播放器 1 傳輸到來所被密碼化之資料。因此，提高安全性。

第 6 圖係為表示對於始源端 (D V D 播放器 1)，不只是個人電腦 2，磁光碟裝置 3 也是作為接收端功能時之處理例。

此情況，在作為接收端 1 的個人電腦 2 之 E E P R O M 5 0，記憶有 I D 1 作為 I D，另外記憶有 license_key 1 作為許可鍵；在於作為接收端 2 之磁光碟裝置 3，也是在 E E P R O M 3 7，記憶有 I D 2 作為 I D，另外記憶有 license_key 2 作為許可鍵。

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明(10)

在於DVD播放器1(始源)與個人電腦2(接收1)之間所進行之步驟S11至步驟S20的處理,由於是與第4圖的步驟S1至步驟S10的處理實質上為同樣的處理,所以其說明省略。

即是,如上述,DVD播放器1,對於個人電腦2進行鑑認處理。然後,在於步驟S21,DVD播放器1,對於磁光碟裝置3,要求ID。在於磁光碟裝置3,在步驟S22介由1394介面36,收訊此ID要求訊號,則該固件30(第10圖),在步驟S23讀出被記憶在EEPROM37之ID(ID2),將此ID從1394介面36,介由1394匯流排11而被傳輸到DVD播放器1。DVD播放器1的固件20,在步驟S24,介由1394介面26,而接受此ID2,則在步驟S25,從下式生成鍵lk2。

$$lk2 = \text{hash}(ID \parallel \text{serviec_key})$$

進而,固件20,在步驟S26運算下式,將在步驟S16所生成之鍵sk,使用在步驟S26所生成之鍵lk2而密碼化,生成已密碼化的資料e2。

然後,在步驟S27,固件20,將此密碼化資料e2,從1394介面26介由1394匯流排11而傳輸到磁光碟裝置3。

在於磁光碟裝置3,在步驟S28,介由1394介

五、發明說明(11)

面36，收訊此密碼化資料 e_2 ，在步驟S29，運算下式，而生成密碼鍵 sk_2' 。

$$sk_2' = \text{Dec}(\text{license_key}_2, e_2)$$

如上述，在於個人電腦2及磁光碟裝置3分別得到密碼鍵 sk_1' ， sk_2' 。這些之值形成為與在DVD播放器1之密碼鍵 sk 同一之值。

在於第6圖的處理例，DVD播放器1，對於個人電腦2及磁光碟裝置3，分別要求個別的ID，使其處理，但能以通報通訊要求ID時，能進行如第7圖所示的處理。

即是，在於第7圖的處理例，在步驟S41，作為始源端之DVD播放器1，對於全部的接收端（此例的情況，個人電腦2及磁光碟裝置3）以通報通訊要求ID。個人電腦2及磁光碟裝置3，分別在步驟S42及步驟S43，接受此ID傳送要求的訊號，則分別在步驟S44及步驟S45，讀出被記憶在EEPROM50或是EEPROM37之ID1或是ID2，將此ID1或是ID2傳輸到DVD播放器1。DVD播放器1，在步驟S46及步驟S47，分別收訊這些ID。

在於DVD播放器，進而在步驟S48，由下式生成密碼鍵 lk_1 。

（請先閱讀背面之注意事項再填寫本頁）

訂

五、發明說明 (12)

$lk1 = \text{hash}(ID1 \parallel \text{serviec_key})$

進而，在於步驟 S 4 9，由下式生成密碼鍵 $lk2$ 。

$lk2 = \text{hash}(ID2 \parallel \text{serviec_key})$

在於 DVD 播放器 1，進而在步驟 S 5 0，生成密碼鍵 sk ，在步驟 S 5 1，如下式所示，密碼鍵 sk ，將鍵 $lk1$ 作為鍵而被密碼化。

$e1 = \text{Enc}(lk1, sk)$

進而，在於步驟 S 5 2，密碼鍵 sk ，將鍵 $lk2$ 作為鍵，根據次式而被密碼化。

$e2 = \text{Enc}(lk2, sk)$

進而，在於步驟 S 5 3， $ID1$ ， $e1$ ， $ID2$ ， $e2$ ，分別如下式所示而被結合，生成密碼化資料 e 。

$e = ID1 \parallel e1 \parallel ID2 \parallel e2$

在於 DVD 播放器 1，進而在步驟 S 5 4，經上述過程所生成之密碼化資料 e ，以通報通訊被傳輸到個人電腦

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明 (13)

2 及磁光碟裝置 3。

在於個人電腦 2 及磁光碟裝置 3，分別在步驟 S 5 5 或是步驟 S 5 6，收訊這些密碼化資料 e。然後，在於個人電腦 2 及磁光碟裝置 3，分別在步驟 S 5 7 或是步驟 S 5 8，進行下式所示之運算，生成密碼鍵 s k 1'，s k 2'。

$$sk1' = \text{Dec}(\text{license_key1}, e1)$$
$$sk2' = \text{Dec}(\text{license_key2}, e2)$$

第 8 圖係為表示使其 1 個的接收端能接受複數個服務（解碼複數個種類之資訊）的情況之處理例。即是，在於此情況，例如作為接收端之個人電腦 2，將複數個許可鍵（license_key1, license_key2, license_key3 等）記憶在 E E P R O M。作為始源端之 D V D 播放器 1，在該 E E P R O M 2 7 記憶複數個服務鍵（service_key1, service_key2, service_key3 等）。此情況，D V D 播放器 1，在步驟 S 8 1 對於作為接收端之個人電腦 2 要求 I D 時，D V D 播放器 1，傳送識別從此處所傳送的資訊（服務）之 service_ID。在於個人電腦 2，在步驟 S 8 2，收訊此 service_ID 時，從被記憶在 E E P R O M 5 0 之複數個許可鍵當中，選擇對應於此 service_ID 之資訊，用此資訊，在步驟 S 9 0 進行解碼處理。其他的動作，與第 4 圖的情況同樣。

（請先閱讀背面之注意事項再填寫本頁）

訂

五、發明說明 (14)

第 9 圖係為表示另外的處理例。在於此例，作為始源端的 DVD 播放器 1，在其 EEPROM 27，記憶 service_key，hash 函數，及疑似亂數產生函數 pRNG。這些則是著作權者所提供，且被秘密的保管。另外，在作為接收端之個人電腦 2 之 EEPROM 50，具有從著作權者所供予的 ID，LK，LK'，函數 G，及疑似亂數產生函數 pRNG。

LK 係為著作權者所作成之特異性亂數；LK' 係為使其滿足而被生成。

$$LK' = G^{-1}(R)$$

$$R = \text{pRNG}(H)(+) \text{pRNG}(LK)$$

$$H = \text{hash}(ID \parallel \text{service-key})$$

然而， G^{-1} 係為意味著 G 的反函數。 G^{-1} 具有若為已知所定的規則，則能簡單地計算，但若為未知時，則不易計算之特徵。作為此樣的函數，可以利用被用於公開密碼鍵之函數。

另外，疑似亂數產生函數，也能使其作為軟體而設置。

DVD 播放器 1 的固件 20，最初在於步驟 S101，對於個人電腦 2 的許可管理 62 要求 ID。個人電腦 2 的許可管理 62，在步驟 S102，接受 ID 要求訊號，則讀出被記憶在 EEPROM 50 的 ID，在步驟

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明(15)

S 1 0 3，將此 I D 傳輸到 D V D 播放器 1。D V D 播放器 1 的固件 2 0，在步驟 S 1 0 4 接受此 I D，則在步驟 S 1 0 5，運算下式

$$H = \text{hash}(ID \parallel \text{service_key})$$

進而，固件 2 0，在步驟 s 1 0 6，生成鍵 s k，在步驟 S 1 0 7，運算下式

$$e = sk(+)pRng(H)$$

然而，A (+) B 係為意味著運算 A 與 B 的排他邏輯和。

即是在疑似亂數產生鍵 p R N G 輸入在步驟 S 1 0 5 所求得的 H 而得到之結果，運算 p R N G (H) 及在步驟 S 1 0 6 所生成之鍵 s k 的每位元之排他邏輯和，而將鍵 s k 暗碼化。

其次，在步驟 S 1 0 8，固件 2 0 將 e 傳輸到個人電腦。

在於個人電腦 2，在步驟 S 1 0 9 收訊此 e，且在步驟 S 1 1 0，運算下式。

$$sk' = e(+)G(LK')(+)pRNG(LK)$$

五、發明說明 (16)

即是運算在從 D V D 播放器 1 所傳輸到來的 e，被記憶在 E E P R O M 5 0 的函數 G，仍然適用被記憶在 E E P R O M 5 0 的 L K' 而得到之值 G (L K')，並且將被記憶在 E E P R O M 5 0 之 L K'，仍然適用於被記憶在 E E P R O M 5 0 之疑似亂數產生函數而得到的結果 p R N G (L K) 之排他邏輯和。

此處，如下式所示，形成為 $s_k = s_k'$

$$\begin{aligned} s_k' &= e(+)G(LK')(+)pRNG(LK) \\ &= s_k(+)pRNG(H)(+)R(+)pRNG(LK) \\ &= s_k(+)pRNG(H)(+)pRNG(H)(+)pRNG(LK)(+)pRNG(LK) \\ &= s_k \end{aligned}$$

經此樣，作為始源端之 D V D 播放器 1 及作為接收端之個人電腦 2，可以共有同一的鍵 s_k ， s_k' 。因可以作成 L K，L K' 只有著作權者，所以接收端為不正常，就是欲作成 L K，L K' 也不能製作，可以更提高安全性。

在於上述，已經使其在於始源端與接收端進行鑑認，但例如在個人電腦 2，通常可以載入任意的應用程式後使用。然且，作為此應用程式，也有使用不當作成之情況。因此，在各應用程式，必須判定否從著作權者得到許可。此處，如第 3 圖所示，在於各應用部 6 1 與許可管理 6 2 之間，也如上述過，可以使其進行鑑認處理。此情況，許

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明(17)

可管理 6 2 形成爲始源端，應用部 6 1 形成爲接收端。

其次，如上述，說明進行鑑認後（進行共有密碼鍵後），用密碼鍵，將從始源端所密碼化之資料傳輸到接收端，在於接收端，解碼此所密碼化的資料時的動作。

如第 10 圖所示，如 DVD 播放器 1，或是磁光碟裝置 3，在於內部的功能未開放給一般使用者之裝置，介由 1 3 9 4 匯流排 1 1 而收授的資料之密碼化及解碼的處理，分別以 1 3 9 4 介面 2 6 或是 1 3 9 4 介面 3 6 而進行。在此密碼化及解碼化，使用時段鍵 S 及時變鍵 i，但此時段鍵 S 及時變鍵 i（正確的是爲了生成時變鍵 i 之鍵 i' ），分別從固件 2 0 或是固件 3 0，供給到 1 3 9 4 介面 2 6 或是 1 3 9 4 介面 3 6。時段鍵 S 係爲以作爲初期值所用之初期值鍵 S_s 及爲攪亂時變鍵 i 所用之攪亂鍵 S_i 而被構成。此初期值鍵 S_s 及攪亂鍵 S_i ，可以使其在於上述過的鑑認所生成之暗碼鍵 $s_k (= s_k')$ 的所定位元數之上位位元及下位位元，而分別構成。此時段鍵 S，在每個時段（例如，每 1 個的電影資訊，或是每 1 次的再生），適當地被更新。對於此點，攪亂鍵 S_i 及從鍵 i 所生成之時變鍵 i，係爲在於 1 個的時段內，頻繁地被更新之鍵；例如，可以使用在所定時間之時刻資訊等。

現今，將從作爲始源端之 DVD 播放器 1 所再生輸出的影像資料，介由 1 3 9 4 匯流排 1 1 而傳輸到磁光碟裝置 3 及個人電腦 2，針對各個解碼。此情況，針對 DVD 播放器 1，在於 1 3 9 4 介面 2 6，用時段鍵 S 及時變鍵

（請先閱讀背面之注意事項再填寫本頁）

訂

五、發明說明(18)

i，進行密碼化處理。針對磁光碟裝置3，在於1394介面36，用時段鍵S及時變鍵i，進行解碼處理。

對於此點，在於個人電腦2，許可管理62，時段鍵S當中，將初期值鍵S_s供給到應用部61，且將攪亂鍵S_i及時變鍵i（正確的是為了生成時變鍵i之鍵i'）供給到1394介面49（連結部分）。然後，在於1394介面49，從攪亂鍵S_i及鍵i'生成時變鍵i，用時變鍵i進行解碼，將該所被解碼的資料，在於應用部61，進而用時段鍵S（正確的是初期值鍵S_s），進行解碼。

此樣，在於個人電腦2，內部匯流排51，因被開放給使用者，所以以1394介面49只進行第1階段的解碼，仍是密碼的狀態。然後，在於應用部61，進而進行第2階段的解碼，成為語體文。由於此因，對於個人電腦2，適切地附加功能，而使其禁止將在於內部匯流排51所收授的資料（語體文）複製到硬碟47或其他裝置。

此樣，在於本發明的實施形態，針對內部匯流排未被開放的CE裝置，用時段鍵S及時變鍵，進行1次密碼化或是解碼處理，但針對內部匯流排已被開放之裝置（個人電腦2等），區分成用時變鍵i之解碼處理，及用時段鍵S之解碼處理而進行解碼處理。此樣，使其可以具有1階段的解碼處理，及分成2階段解碼處理之兩者，必須使其成立下式。

（請先閱讀背面之注意事項再填寫本頁）

訂

線

1

五、發明說明 (19)

$$\text{Dec}(S, \text{Dec}(I, \text{Enc}(\text{algo}(S+I), \text{Data}))) = \text{Data}$$

然而，在於上述式， $\text{algo}(S+i)$ 係為表示在所定的運算輸入時段鍵 S 及時變鍵 i 而得到的結果。

第 11 圖係為表示滿足上述式之 1394 介面 26 的構成例。在於此構成例，以加法產生器 71 所生成之 m 位元的資料，被供給到收縮產生器 73。另外，LFSR (Linear Feedback Shift Register) 2 輸出 1 位元的資料，供給到收縮產生器 73。收縮產生器 73，係為對應於 LFSR 72 的輸出，而選擇加法產生器 71 的輸出，將所選擇的資料作為密碼鍵而輸出到加算器 74。加算器 74 係為加算所輸入的語體文 (傳輸到 1394 匯流排 11 之 m 位元的資料)，及由收縮產生器 73 所供給的 m 位元的資料 (密碼鍵)，將所加算的結果作為語體文 (所被密碼化的資料)，而輸出到 1394 匯流排 11。

加算器 74 的加算處理，係為意味著以 $\text{mod } 2^m$ (m 為冪次)，加算收縮產生器 73 的輸出及語體文。換言之，加算 m 位元的同類資料，輸出忽視轉入之加算值。

第 12 圖係為表示第 11 圖所示的 1394 介面 26 之更詳細構成例。從固件 20 所輸出的時段鍵 S 當中，初期值鍵 S_s ，介由加算器 81 而被傳輸到暫存器 82 且被保持。此初期值鍵 S_s ，例如以 55 字元 (1 字元具有 8 位元至 32 位元的寬度) 而被構成。另外，從固件 20 所供給的時段 S 當中的例如以 LSB 側的 32 位元而被構成

(請先閱讀背面之注意事項再填寫本頁)

訂

總

五、發明說明(20)

之攪亂鍵 S_i ，被保持在暫存器 8 5。

在暫存器 8 4 被保持有鍵 i' 。此鍵 i' ，例如介由 1 3 9 4 匯流排 1 1 而每次傳送 1 個組套，2 位元的鍵 i' 被供給到暫存器 8 4，1 6 組套分的 (3 2 位元分的) 鍵 i' 被保持在暫存器 8 4 時，以加算器 8 6，而與被保持在暫存器 8 5 之 3 2 位元的攪亂鍵 S_i 加算，作為最終的時變鍵 i 而被供給到加算器 8 1。加算器 8 1，係為加算當時被保持在暫存器 8 2 之值及由加算器 8 6 所供給的時變鍵 i ，將其加算結果供給到暫存器 8 2 且使其保持。

暫存器 8 2 的字元之位元數，例如為 8 位元時，因由加算器 8 6 所輸出的時變鍵 i 為 3 2 位元，所以 4 分割時變鍵 i 後使其將各 8 位元加算到暫存器 8 2 的所定位址 (0 ~ 5 4) 之文字。

經此樣，在暫存器 8 2，最初被保持有初期值鍵 S_s ，但其後，此值係為在每次傳輸 1 6 組套分的密碼文，以時變鍵 i 而被更新。

加算器 8 3，係為選擇被保持在暫存器 8 2 之 5 5 位元當中的所定 2 文字 (第 1 2 圖所示之時間的情況為位址 2 3 及位址 5 4 的字元)，加算該所選擇的 2 位元後，輸出至收縮產生器 7 3。另外，此加算器 8 3 的輸出，在第 1 2 圖所示的時間，則是被傳輸到暫存器 8 2 的位址 0，取代之前的保持值而被保持。

然後，在於次個時間，被供給到加算器 8 3 之暫存器

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明(21)

8 2 的 2 位元之位址，從位址 5 4 及位址 2 3，只 1 位元分，朝圖中上方分別移動至位址 5 3 及位址 2 2，以加算器 8.3 的輸出而被更新的位址，也是圖中移動至更上方的位址。不過，比位址 0 還上方的位址因未存在，所以此情況，移動至位址 5 4。

然而，在加算器 8 1，8 3，8 6 也能使其運算排他邏輯和。

L F S R 7 2，例如如第 1 3 圖所示，以加算 n 位元的移位暫存器 1 0 1 及移位暫存器 1 0 1 的 n 位元當中的所定位元（暫存器）之值的加算器 1 0 2 而被構成。移位暫存器 1 0 1，將由加算器 1 0 2 所供給的位元，保持在圖中最左側的暫存器 b_n ，則將至此被保持在該處的資料移位到右側的暫存器 b_{n-1} 。暫存器 b_{n-1} ， b_{n-2} ，……也進行同樣的處理。然後，進而在次個時間，將以加算器 1 0 2 加算各位元之值所得之值，再度使其保持在圖中最左側的位元 b_n 。依順返復以上的動作，從圖中最右側的暫存器 b_1 依順輸出每 1 位元。

第 1 3 圖係為一般的構成例，但例如，更具體地，可以如第 1 4 圖所示構成 L F S R 7 2。在於此構成例，以 3 1 位元構成移位暫存器 1 0 1，以加算器 1 0 2 加算該圖中右端的暫存器 b_1 之值及左端的暫存器 b_{31} 之值，所被加算的結果使其回歸到暫存器 b_{31} 。

由 L F S R 7 2 所輸出的 1 位元資料為邏輯 1 時，條件判定部 9 1，將由加法產生器 7 1 的加算器 8 3 所供給

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明(22)

之 m 位元的資料原樣傳輸到 F I F O 9 2 且使其保持。對於此點，由 L F S R 7 2 所供給的 1 位元之資料為邏輯 0 時，條件判定部 9 1，未接受由加算器 8 3 所供給的 m 位元之資料，使其中斷密碼化處理。經此樣，在收縮產生器 7 3 的 F I F O 9 2，只選擇以加法產生器 7 1 所生成之 m 位元的資料當中，L F S R 7 2 輸出邏輯 1 的時間之資料且被保持。

以 F I F O 9 2 所保持的 m 位元之資料，作為密碼鍵，而被供給到加算器 7 4，加算到應被傳輸的語體文之資料（從 D V D 的再生資料），生成密碼文。

所被密碼化之資料，從 D V D 播放器 1 介由 1 3 9 4 匯流排 1 1 而被供給到磁光碟裝置 3 及個人電腦 2。

磁光碟裝置 3，在於 1 3 9 4 介面，為了解碼從 1 3 9 4 匯流排 1 1 所收訊的資料，而具有如第 1 5 圖所示之構成。在於此構成例，加法產生器 1 7 1 所輸出的 m 位元之資料，及 L F S R 所輸出的 1 位元之資料被供給到收縮產生器 1 7 3。然後，收縮產生器 1 7 3 所輸出的 m 位元之鍵，被供給到減算器 1 7 4。減算器 1 7 4，從密碼文減算由收縮產生器 1 7 3 所供給之鍵，而解碼語體文。

即是第 1 5 圖所示之構成係為與第 1 1 圖所示的構成基本上為同樣的構成；在第 1 1 圖的加算器 7 4，只有變更成減算器 1 7 4 之點為相異。

第 1 6 圖係為表示第 1 5 圖所示的構成之更詳細成例

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明(23)

。此構成基本上也是與第12圖所示的構成同樣的構成，但在第12圖之加算器74被變更成減算器174。其他的加法產生器171，LFSR172，收縮產生器173，加算器181，暫存器182，加算器183，暫存器184，185，加算器186，條件判定部191，FIFO192等係為對應於在第12圖的加法產生器71，LFSR72，收縮產生器73，加算器81，暫存器82，加算器83，暫存器84，85，加算器86，條件判定部91，及FIFO92。

因此，其動作基本上是與第12圖所示的情況相同，所以其說明省略，但在於第16圖，由收縮產生器173的FIFO192所輸出之m位元之鍵，在於減算器174，從暗碼文減算後而解碼語體文。

如上述，在於1394介面36，用時段鍵S（初期值鍵S_s及攪亂鍵S_i）及時變鍵i，而解碼1次密碼化資料。

對於此點，如上述，在於個人電腦2，針對1394介面49及應用部61，分別分成2階段而進行解碼。

第17圖係為表示在於1394介面49，進行解碼的情況之構成例。其基本構成係為與第15圖所示的情況同樣。即是在於此情況也是以加法產生器271，LFSR272，收縮產生器273及減算器274，構成1394介面49；這些係為與在第15圖的加法產生器171，LFSR172，收縮產生器173，及減算

（請先閱讀背面之注意事項再填寫本頁）

訂

線

五、發明說明(24)

器，基本上是同樣的構成。不過，在於第17圖的構成例，對於加法產生器271，作為為了從許可管理62，生成時變鍵 i 之鍵 i' ，及時段鍵 S 當中，為了攪亂時變鍵 i 之攪亂鍵 S_i ，係為供給與在第15圖的情況同樣的鍵，但作為初期值鍵 S_s ，係為供給全部的位元為0之單位元。

即是如第18圖所示，因初期值鍵 S_s 的全部位元設為0，所以實質上，與初期值鍵 S_s 為存在的情況同樣地，根據時變鍵 i 而生成密碼鍵。其結果，在於減算器274，根據密碼文的時變鍵 i 只進行解碼。因尚未根據初期值鍵 S_s 進行解碼，所以此解碼結果所得的結果之資料，未形成為完全的語體文，而是形成為密碼文的狀態。因此，從內部匯流排51載入此資料，記錄至硬碟47，或其他記錄媒體，也無法原樣利用該資料。

然且，如上述，在於1394介面49，硬體式的根據時變鍵 i 而軟體式的解碼所被解碼的資料之應用部61的構成，係為如第19圖所示，以加法產生器371，LFSR372，收縮產生器373及減算器374而被構成。其基本構形成為與第15圖所示的加法產生器171，LFSR172，收縮產生器173及減算器174同樣的構成。

不過，時段鍵 S 當中，初期值鍵 S_s ，係為與第15圖的情況同樣地，供給一般的初期值鍵，但為了生成時變鍵 i 之攪亂鍵 S_i 及鍵 i ，分別是全部的位元為0之單位

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明(25)

元的資料。

其結果，在第20圖表示其詳情（其加法產生器371及FFO392，係為對應於第16圖的加法產生器171及F1FO192），被保持在暫存器384之鍵 i 及被保存在暫存器385之攪亂鍵 S_i ，由於全部的位元為0，所以加算器386所輸出的時變鍵 i 也是全部的位元形成為0，實質上進行與時變鍵 i 未存在的情況同樣的動作。即是只根據初期值鍵 S_s 生成密碼鍵。然後，在於減算器374，根據經此過程所生成之密碼鍵，密碼文被解碼成語體文。如上述，此密碼文，因在於1394介面49，根據時變鍵 i 而進行第1階段的解碼，所以在此處，根據初期值鍵 S_s 進行第2階段的解碼，而可以得到完全的語體文。

在於磁光碟裝置3，經上述過程而解碼密碼文，則CPU31，將所被解碼的資料供給到驅動器35，且使其記錄至磁光碟。

另則，在於個人電腦2，CPU41（應用部61），將經上述所被解碼的資料，例如供給到硬碟47且使其記錄。在於個人電腦2，可以以擴充埠48連接所定的連接埠，而監視在內部匯流排51所收授的資料，但可以最終的解碼被傳輸到內部匯流排51的資料，就是為應用部61，所以可以監視擴充埠48，以1394介面，根據時變鍵 i 進行解碼之資料（尚未根據時段鍵 S 進行解碼之資料，也無法監視完全的恢復成語體文之資料。因此，可

（請先閱讀背面之注意事項再填寫本頁）

訂

五、發明說明 (26)

以防止不當的複製。

然而，時段鍵的共有，例如也能使用 Diffie-Hellman 法等而使其進行。

然而，另外例如在個人電腦 2 之 1 3 9 4 介面 4 9 或是應用部 6 1 的處理能力較低，無法進行解碼處理時，若在於始源端側，使其以單位元構成時段鍵與時變鍵的其中 1 個，或是兩者；在於接收端側，也是以單位元使用這些鍵，則實施上未使用時段鍵及時變鍵，形成爲能收授資料。不過，若爲此樣，則恐會增高資料的不當複製之疑慮。

應用部 6 1 其資料，若爲不正複製的資料時，恐會有不當複製所被解碼的資料，但如上述，若使其以許可管理 6 2 鑑認應用部 6 1，則能防止不當複製。

作爲此情況的鑑認方法，可以利用共通鍵密碼方式或是公開鍵密碼方式之數字式署名。

以上的第 1 1 圖，第 1 2 圖，第 1 5 圖及第 2 0 圖所示之構成，係爲滿足準同形 (homomorphism) 的關係之構成。即是鍵 K_1 ， K_2 爲伽羅瓦 (Galois) 領域 G 的要素時，兩者的群運算結果， K_1 ， K_2 也形成爲伽羅瓦領域 G 的要素。然且，進而針對所定的函數 H ，成立下式。

$$H(K_1 \cdot K_2) = H(K_1) \cdot H(K_2)$$

第 2 1 圖係爲進而表示 1 3 9 4 介面 2 6 的其他構成例。在於此構成例，使其時段鍵 S 被供給到

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (27)

L F S R 5 0 1 至 5 0 3 ， 且 被 初 期 設 定 。

L F S R 5 0 1 至 5 0 3 之 幅 寬 的 n_1 至 n_3 ， 分 別 以 2 0 位 元 程 度 ， 各 別 的 幅 寬 n_1 至 n_3 為 相 互 地 成 為 因 素 而 被 構 成 。 因 此 ， 例 如 時 段 鍵 S 當 中 ， 例 如 上 位 n_1 位 元 被 初 期 設 定 在 L F S R 5 0 1 ， 其 次 的 上 位 n_2 位 元 被 初 期 設 定 在 L F S R 5 0 2 ， 進 而 其 次 的 上 位 n_3 位 元 初 期 設 定 在 L F R 5 0 3 。

L F S R 5 0 1 至 5 0 3 ， 由 計 時 功 能 5 0 6 ， 例 如 輸 入 邏 輯 1 的 能 啓 動 訊 號 時 ， 只 m 位 元 進 行 移 位 動 作 ， 輸 出 m 位 元 的 資 料 。 m 之 值 例 如 可 以 設 為 8 ， 1 6 ， 3 2 ， 4 0 。

L F S R 5 0 1 及 L F S R 5 0 2 之 輸 出 ， 被 輸 入 到 加 算 器 5 0 4 ， 且 被 加 算 。 加 算 器 5 0 4 的 加 算 值 當 中 ， 載 體 成 分 ， 被 供 給 到 計 時 功 能 5 0 6 ； s u m 成 分 ， 被 供 給 到 加 算 器 5 0 5 ， 與 L F S R 5 0 3 的 輸 出 加 算 。 加 算 器 5 0 5 的 載 體 成 分 ， 被 供 給 到 計 時 功 能 5 0 6 ； s u m 成 分 ， 被 供 給 到 排 他 邏 輯 和 電 路 5 0 8 。

計 時 功 能 5 0 6 ， 由 於 是 由 加 算 器 5 0 4 及 加 算 器 5 0 5 所 供 給 的 資 料 組 合 為 0 0 ， 0 1 ， 1 0 ， 1 1 的 其 中 1 個 ， 所 以 對 應 於 這 些 ， 而 對 L F S R 5 0 1 至 5 0 3 ， 輸 出 0 0 0 至 1 1 1 的 其 中 1 個 之 組 合 資 料 。

L F S R 5 0 1 至 5 0 3 ， 係 為 在 輸 入 邏 輯 1 時 ， 進 行 m 位 元 的 移 位 動 作 ， 且 輸 出 新 的 m 位 元 之 資 料 ； 輸 入 邏 輯 0 時 ， 輸 出 與 前 次 所 輸 出 的 情 況 同 一 m 位 元 之 資 料 。

(請先閱讀背面之注意事項再填寫本頁)

訂

線

五、發明說明 (28)

排他邏輯和電路 5 0 8，係為運算加算器 5 0 5 所輸出的 s u m 成分及被保持在暫存器 5 0 7 的時變鍵 i 之排他邏輯和，將其運算結果輸出至排他邏輯和電路 5 0 9。排他邏輯和電路 5 0 9，係為運算所被輸入的語體文，及由排他邏輯和電路 5 0 8 所輸入之密碼鍵的排他邏輯和，將運算結果作為密碼後輸出。

第 2 2 圖係為表示在磁光碟裝置 3 的 1 3 9 4 介面 3 6 之構成例。在此構成例之 L F S R 6 0 1 至排他邏輯和電路 6 0 9，係為與第 2 1 圖的 L F S R 5 0 1 至排他邏輯和 5 0 9 同樣的構成。因此，該動作基本上也是同樣，所以省略其說明。不過，對於在於第 2 1 圖的構成例，進行密碼化處理；在於第 2 2 圖的構例，則是進行解碼處理。

第 2 3 圖係為表示個人電腦 2 的 1 3 9 4 介面 4 9 之構成例。在此構成例之 L F S R 7 0 1 至排他邏輯和電路 7 0 9，也是與在第 2 2 圖的 L F S R 6 0 1 至排他邏輯和電路 6 0 9 同樣的構成。不過，被初期設定在 L F S R 7 0 1 至 7 0 3 之時段鍵 S，係為全部的位元為 0 單位元。因此，此情況，實質上只對應於被保持在暫存器 7 0 7 之時變鍵 i 而進行解碼化處理。

第 2 4 圖係為表示個人電腦 2 的應用部 6 1 之構成例。在此構成例之 L F S R 8 0 1 至排他邏輯和電路 8 0 9，係為與在第 2 圖之 L F S R 6 0 1 至排他邏輯和電路 6 0 9 基本上是一樣的構成。不過，被輸入至暫存器

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明(29)

8 0 7 之時變鍵 i，只有全部的位元為 0 單位之點為相異。因此，此構成例的情況，只根據時段鍵 S 而生成密碼鍵，進行解碼處理。

然而，第 19 圖，第 20 圖及第 24 圖所示之處理，由於是在於應用部 61 而進行，因而是軟性式的處理。

在於上述，將 DVD 播放器作為始源端，將個人電腦 2 及磁光碟裝置 3 作為接收端，但將任何的裝置作為始源端或是接收端為任意。

另外，連接各電子機器之外部匯流排，也不限於 1394 匯流排，可以利用種種的匯流排，連接至該匯流排之電子機器，也是不限於上述過之例，任意的裝置皆可。

[發明效果]

如上述，依據申請專利第 1 項及申請專利第 9 項之密碼化方法，由於用第 1 鍵，及將資料密碼化時，在所定時間所被變更的第 2 鍵而使其生成暗碼鍵，所以能更安全地進行密碼化。

依據申請專利第 10 項及申請專利第 13 項，由於用第 1 鍵，及解碼資料時，在所定時間所被變更的第 2 鍵而使其生成密碼鍵，所以能更安全地解碼所被密碼化的資料。

依據申請專利第 14 項之資訊處理系統及申請專利第 15 項之資訊處理方法，在於功能變更未開放給使用者之

(請先閱讀背面之注意事項再填寫本頁)

訂



五、發明說明 (30)

第 1 資訊處理裝置，用第 1 鍵，及解碼資料時，在所定時間所被變更的第 2 鍵，而使其生成密碼鍵；在於功能變更被開放給使用者之第 2 資訊處理裝置，用第 1 鍵及第 2 鍵的一方，生成之第 1 密碼鍵，解碼所被密碼化的資料，用第 1 鍵及第 2 鍵的他方所生成之第 2 密碼鍵，進而使其解碼該所被解碼的資料，所以能實現更安全的資訊處理系統。

依據申請專利第 1 6 項之資訊處理裝置及申請專利第 1 7 項之資訊處理方法，由於以軟體程式使其生成第 1 鍵，及解碼資料時，在所定時間所被變更的第 2 密碼鍵，所以能在每個應用程式進行解碼，且能更確實地防止不當的複製。

[圖面之簡單說明]

第 1 圖係為表示適用本發明的資訊處理系統構成例之方塊圖。

第 2 圖係為表示第 1 圖的 D V D 播放器 1，個人電腦 2，及磁光碟裝置的內部構成例之方塊圖。

第 3 圖係為說明鑑認處理之圖。

第 4 圖係為說明鑑認處理之時間圖。

第 5 圖係為表示 node_unique_ID 的格式之圖。

第 6 圖係為說明其他的鑑認處理之時間圖。

第 7 圖係為說明另外的鑑認處理之時間圖。

第 8 圖係為說明其他的鑑認處理之時間圖。

五、發明說明(31)

第9圖係為說明其他的鑑認處理之時間圖。

第10圖係為說明密碼化處理之方塊圖。

第11圖係為表示第10圖1394介面26的構成例之方塊圖。

第12圖係為表示第11圖1394介面26的更詳細構成例之方塊圖。

第13圖係為表示第12圖LFSR72的更詳細構成例之方塊圖。

第14圖係為表示第13圖LFSR72的更具體構成例之方塊圖。

第15圖係為表示第10圖1394介面36的構成例之方塊圖。

第16圖係為表示第15圖1394介面36的更詳細構成例之方塊圖。

第17圖係為表示第10圖1394介面49的構成例之方塊圖。

第18圖係為表示第17圖1394介面49的更詳細構成例之方塊圖。

第19圖係為表示第10圖應用部61的構成例之方塊圖。

第20圖係為表示第19圖應用部61的更詳細構成例之方塊圖。

第21圖係為表示第10圖1394介面26的其他構成例之方塊圖。

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明(32)

第22圖係為表示第10圖1394介面36的其他構成例之方塊圖。

第23圖係為表示第10圖1394介面36的其他構成例之方塊圖。

第24圖係為表示第10圖應用部61的其他構成例之方塊圖。

[圖號說明]

- 1 : DVD 播放器
- 2 : 個人電腦
- 3 : 磁光碟裝置
- 11 : 1394 匯流排
- 20 : 固件
- 21 : CPU
- 25 : 驅動器
- 26 : 1394 介面
- 27 : EEPROM
- 31 : CPU
- 35 : 驅動器
- 36 : 1394 介面
- 37 : EEPROM
- 41 : CPU
- 47 : 硬體
- 48 : 擴充埠

(請先閱讀背面之注意事項再填寫本頁)

訂

五、發明說明 (33)

4 9 : 1 3 9 4 介 面

5 0 : E E P R O M

5 1 : 內 部 匯 流 排

6 1 : 應 用 部

6 2 : 許 可 管 理

(請先閱讀背面之注意事項再填寫本頁)

訂

線

六、申請專利範圍

- 1 . 一種密碼化裝置，其特徵為具備：
用密碼鍵將資料密碼化之密碼化手段，及
產生第 1 鍵之第 1 鍵產生手段，及
當資料密碼化時，產生在所定時間所被變更的第 2 鍵
之第 2 鍵產生手段，及
用前述第 1 鍵及第 2 鍵，生成前述密碼鍵之生成手段
。
- 2 . 如申請專利範圍第 1 項之密碼化裝置，其中前述
生成手段係為生成準同形的密碼鍵。
- 3 . 如申請專利範圍第 1 項之密碼化裝置，其中前述
生成手段係為個別使用構成前述密碼鍵的第 1 密碼鍵及第
2 密碼鍵，而依順解碼所被密碼化的資料，生成正確解碼
結果所得到的密碼鍵。
- 4 . 如申請專利範圍第 1 項之密碼化裝置，其中前述
生成手段，係為在以前述第 1 鍵作為初期值之值，加算第
2 鍵，而生成前述密碼鍵。
- 5 . 如申請專利範圍第 4 項之密碼化裝置，其中前述
第 1 鍵係為比前述第 2 鍵還多的位元數；前述生成手段，
係為將前述第 2 鍵加算到前述第 1 鍵的所定位置之位元，
抽出加算結果的所定位置之位元，進而加算到所抽出的位
元，而生成前述密碼鍵。
- 6 . 如申請專利範圍第 5 項之密碼化裝置，其中前述
生成手段，係為以進而加算到前述所抽出的位元而得到之
結果，進而更新前述加算結果的所定位元。

六、申請專利範圍

7 . 如申請專利範圍第 6 項之密碼化裝置，其中前述生成手段，係為從進而加算到前述所抽出的位元而得到的結果當中，在所定的時間選擇所定的位元，而生成前述密碼鍵。

8 . 如申請專利範圍第 1 項之密碼化裝置，其中具備將以前述密碼鍵所密碼化之資料，介由匯流排而傳輸到其他裝置之傳輸手段。

9 . 一種密碼化方法，其特徵為具備：

用密碼鍵將資料密碼化之密碼化步驟，及

產生第 1 鍵之第 1 產生步驟，及

將資料密碼化時，產生在所定時間所被變更的第 2 鍵之第 2 產生步驟，及

用前述第 1 鍵及第 2 鍵，生成前述密碼鍵之生成步驟。

10 . 一種解碼裝置，其特徵為具備：

收訊所被密碼化的資料之收訊手段，及

用密碼鍵，解碼前述所收訊的資料之解碼手段，及

產生第 1 鍵之第 1 鍵產生手段，及

解碼資料時，產生在所定時間所被變更的第 2 鍵之第 2 產生手段，及

用前述第 1 鍵及第 2 鍵，生成前述密碼鍵之生成手段。

11 . 如申請專利範圍第 10 項之解碼裝置，其中前述生成手段，具備：

六、申請專利範圍

用前述第 1 鍵及第 2 鍵的一方，生成第 1 密碼鍵之第 1 生成手段，及

用前述第 1 鍵及第 2 鍵的他方，生成第 2 密碼鍵之第 2 生成手段；

前述解碼手段，具備：

用前述第 1 密碼鍵，解碼前述所被密碼化的資料之第 1 解碼手段，及

用前述第 2 密碼鍵，進而解碼以前述第 1 解碼手段而被解碼的資料之第 2 解碼手段。

1 2 . 如申請專利範圍第 1 1 項之解碼裝置，其中前述第 2 解碼手段，係為以處理所被解碼的資料之應用軟體而被構成。

1 3 . 一種解碼方法，其特徵為具備：

收訊所被密碼化的資料之收訊步驟，及

用密碼鍵解碼前述所收訊的資料之解碼步驟，及

產生第 1 鍵之第 1 產生步驟，及

當解碼資料時，產生在所定時間所被變更的第 2 鍵之第 2 產生步驟，及

用前述第 1 鍵及第 2 鍵，生成前述密碼鍵之生成步驟。

1 4 . 一種資訊處理系統，係為針對以介由匯流排，相互連接的複數個資訊處理裝置，而被構成之資訊處理系統；其特徵為：

前述資訊處理裝置，係為以功能變更未開放給使用者

89105738

A8
B8
C8
D8

六、申請專利範圍

之第 1 資訊處理裝置，及功能變更開放給使用者之第 2 資訊處理裝置等而被構成；

前述第 1 資訊處理裝置，具備：

收訊所被密碼化的資料之第 1 收訊手段，及

用密碼鍵，解碼前述第 1 收訊手段所收訊的資料之第

1 解碼手段，及

產生第 1 鍵之第 1 產生手段，及

當解碼資料時，產生在所定時間所被變更的第 2 鍵之

第 2 產生手段，及

用前述第 1 產生手段所產生的第 1 鍵及前述第 2 產生手段所產生的第 2 鍵，生成前述密碼鍵之第 1 生成手段；

前述第 2 資訊處理裝置，具備：

收訊所被密碼化的資料之第 2 收訊手段，及

產生第 1 鍵之第 3 產生手段，及

當解碼資料時，產生在所定時間所被變更的前述第 2

鍵之第 4 產生手段，及

用前述第 3 產生手段所產生的第 1 鍵及前述第 4 產生手段所產生的第 2 鍵其一方，生成第 1 密碼鍵之第 2 生成手段；及

用前述第 3 產生手段所產生的第 1 鍵及前述第 4 產生手段所產生的第 2 鍵其他方，生成第 2 密碼鍵之第 3 生成手段；及

用前述第 1 密碼鍵，解碼前述收訊手段所收訊的密碼化資料之第 2 解碼手段，及

六、申請專利範圍

用前述第 2 密碼鍵，進而解碼以前述第 2 解碼手段而被解碼的資料之第 3 解碼手段。

15. 一種資訊處理方法，係為針對以介由匯流排，相互連接的複數個資訊處理裝置之資訊處理系統的資訊處理方法；其特徵為：

前述資訊處理裝置，係為以功能變更未被開放給使用者之第 1 資訊處理裝置，及功能變更開放給使用者之第 2 資訊處理裝置等而被構成；

前述第 1 資訊處理裝置，具備：

收訊所被密碼化的資料之第 1 收訊步驟，及

用密碼鍵，解碼在前述第 1 收訊步驟所收訊的資料之第 1 解碼步驟，及

產生第 1 鍵之第 1 產生步驟，及

當解碼資料時，產生在所定時間所被變更的第 2 鍵之第 2 產生步驟，及

用在前述第 1 產生步驟所產生的第 1 鍵及在前述第 2 產生步驟所產生的第 2 鍵，生成前述密碼鍵之第 1 生成步驟；

前述第 2 資訊處理裝置，具備：

收訊所被密碼密化的資料之第 2 收訊步驟，及

產生第 1 鍵之第 3 產生步驟，及

當解碼資料時，產生在所定時間所被變更的前述第 2 鍵之第 4 產生步驟，及

用在前述第 3 產生步驟所產生的第 1 鍵及在前述第 4

(請先閱讀背面之注意事項再填寫本頁)

表

訂

像

六、申請專利範圍

產生步驟所產生的第 2 鍵其一方，生成第 1 密碼鍵之第 2 生成步驟；及

用在前述第 3 產生步驟所產生的第 1 鍵及前述第 4 產生步驟所產生的第 2 鍵其他方，生成第 2 密碼鍵之第 3 生成步驟；及

用前述第 1 密碼鍵，解碼在前述第 2 收訊步驟所收訊的被密碼化的資料之第 2 解碼步驟，及

用前述第 2 密碼鍵，進而解碼在前述第 2 解碼步驟所被解碼的資料之第 3 解碼步驟。

1 6 . 一種資訊處理裝置，其特徵為具備：

收訊介由匯流排而傳輸到來的資料之收訊手段，及

從前述收訊手段所收訊的資料，生成第 1 密碼鍵及當解碼資料時，在所定時間所被變更的第 2 密碼鍵之軟體程式所形成之生成手段，及

用前述生成手段所生成的第 1 密碼鍵及第 2 密碼鍵其一方，解碼前述收訊手段所收訊的被密碼化資料之第 1 解碼手段，及

用前述生成手段所生成的第 1 密碼鍵及第 2 密碼鍵其他方，進而解碼以前述解碼手段所被解碼的資料後作處理之軟體程式所形成之第 2 解碼手段。

1 7 . 一種資訊處理方法，其特徵為具備：

收訊介由匯流排而傳輸到來的資料之收訊步驟，及

從在前述收訊步驟所收訊的資料，生成第 1 密碼鍵及當解碼資料時，在所定時間所被變更的第 2 密碼鍵之軟體

(請先閱讀背面之注意事項再填寫本頁)

訂

線

六、申請專利範圍

程式所形成之生成步驟，及

用在前述生成步驟所生成的第 1 密碼鍵及第 2 密碼鍵
其一方，解碼在前述收訊步驟所收訊的被密碼化的資料之
第 1 解碼步驟，及

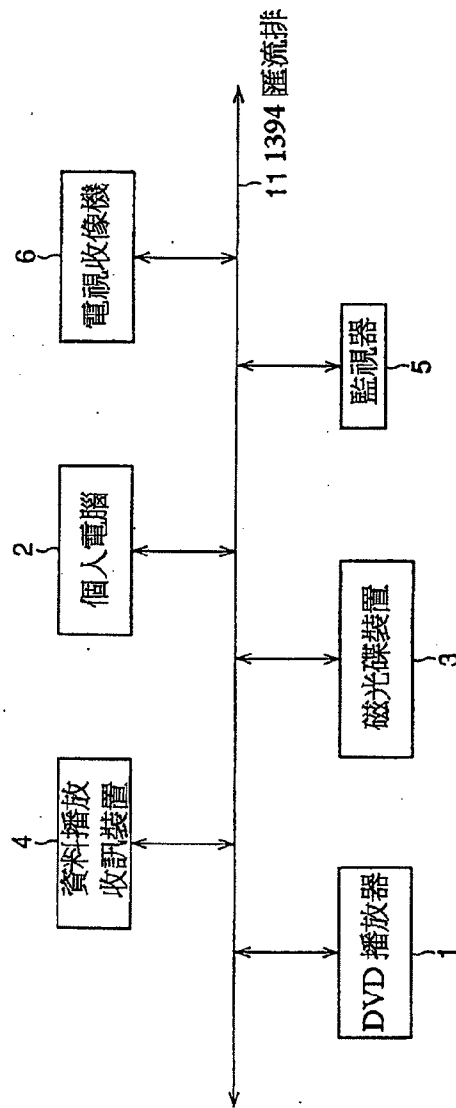
用在前述生成步驟所生成的第 1 密碼鍵及第 2 密碼鍵
其他方，進而解碼在前述第 1 解碼步驟所被解碼的資料後
作處理之軟體程式所形成之第 2 解碼步驟。

(請先閱讀背面之注意事項再填寫本頁)

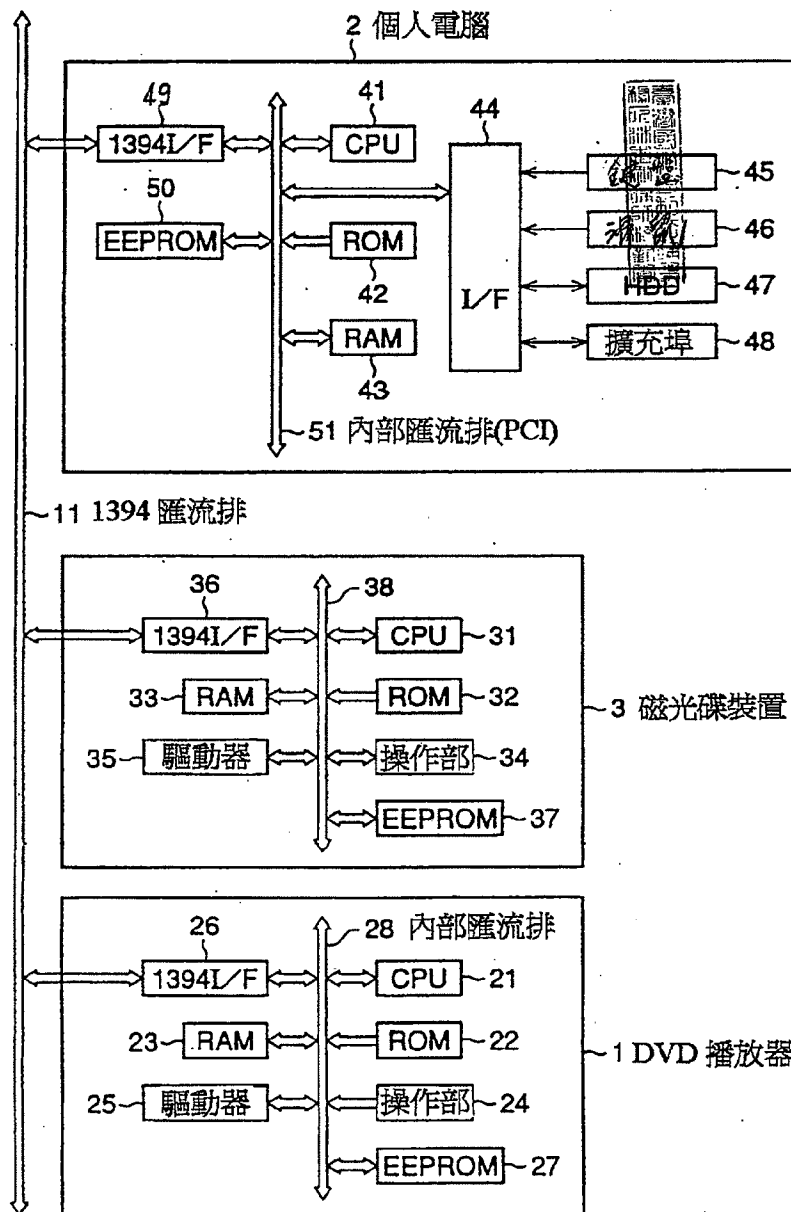
87105738

(1 / 23)

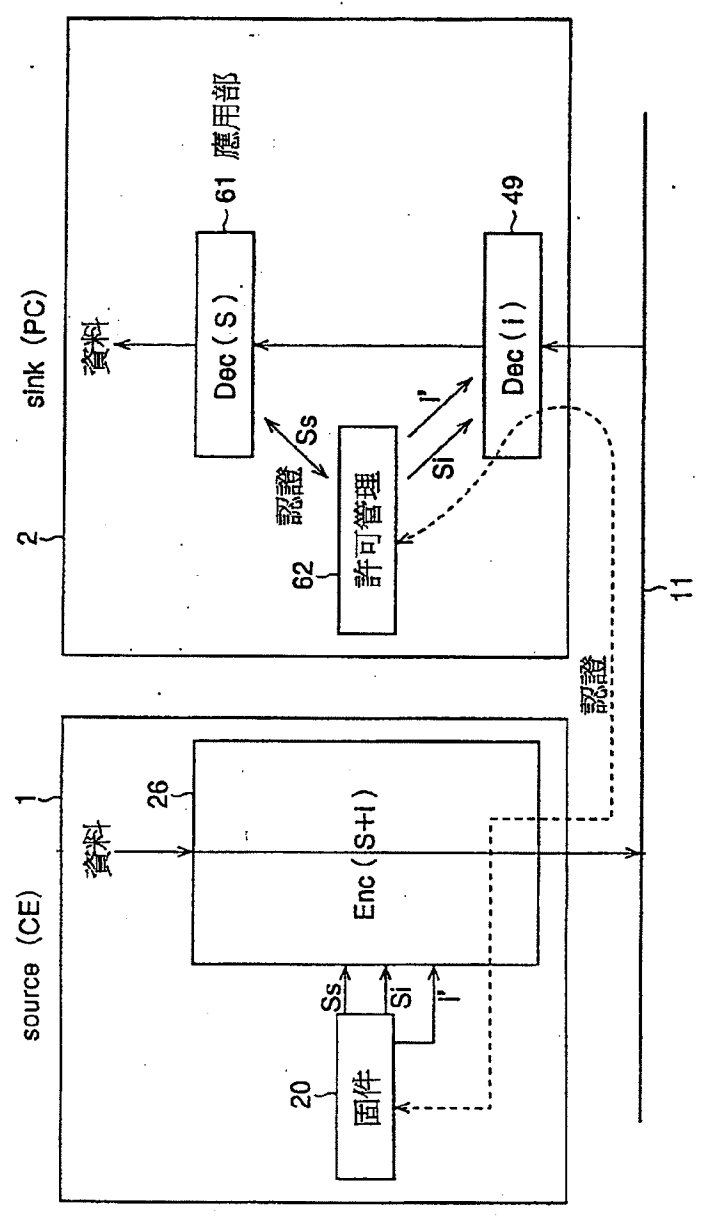
731163



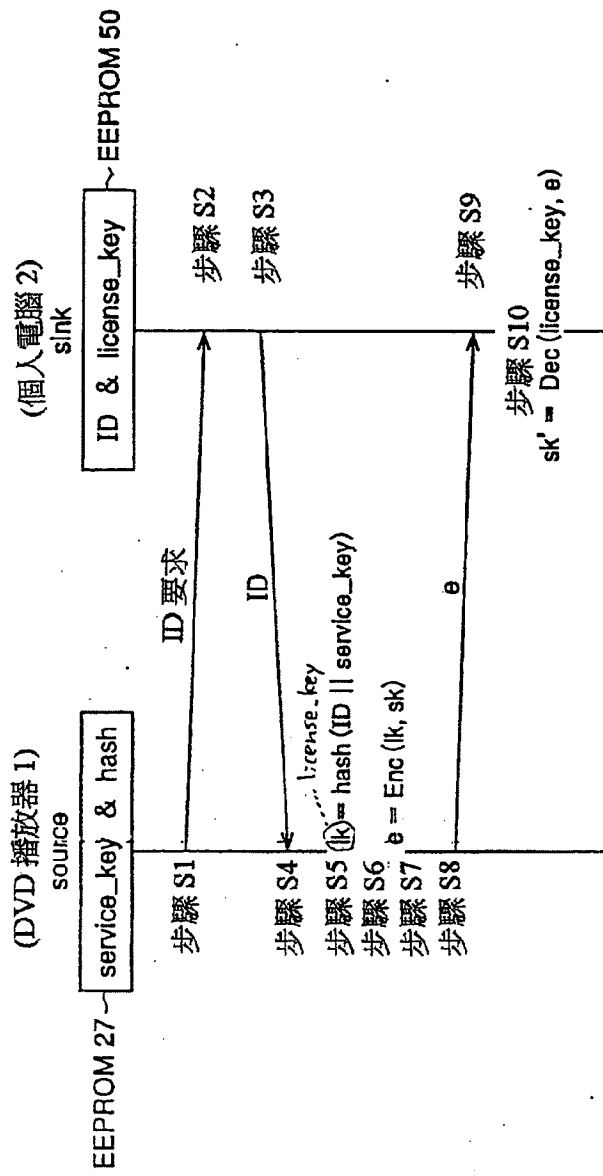
第 1 圖



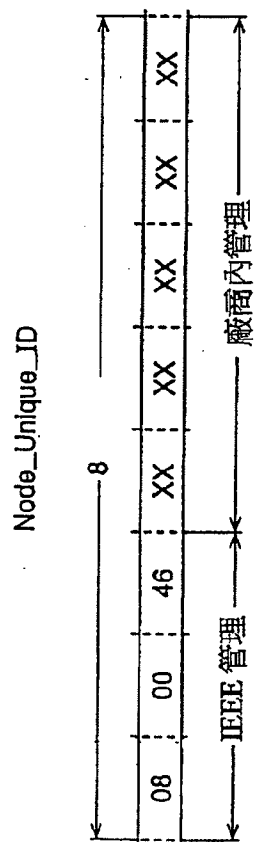
第 2 圖



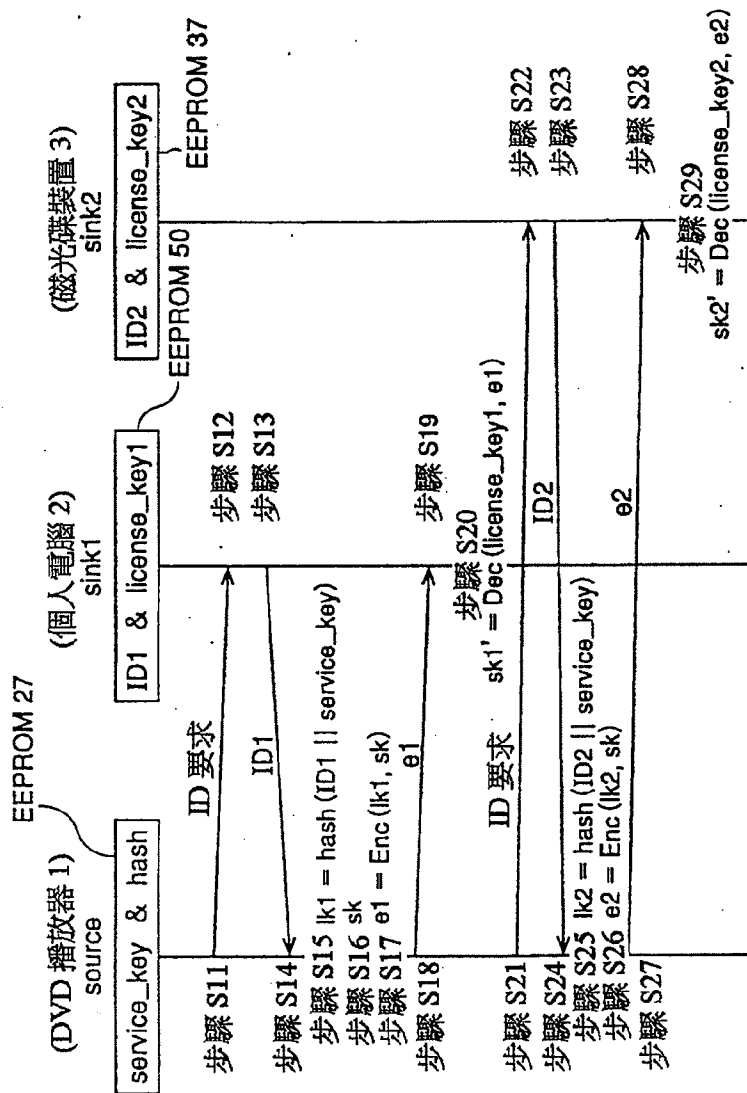
第 3 圖



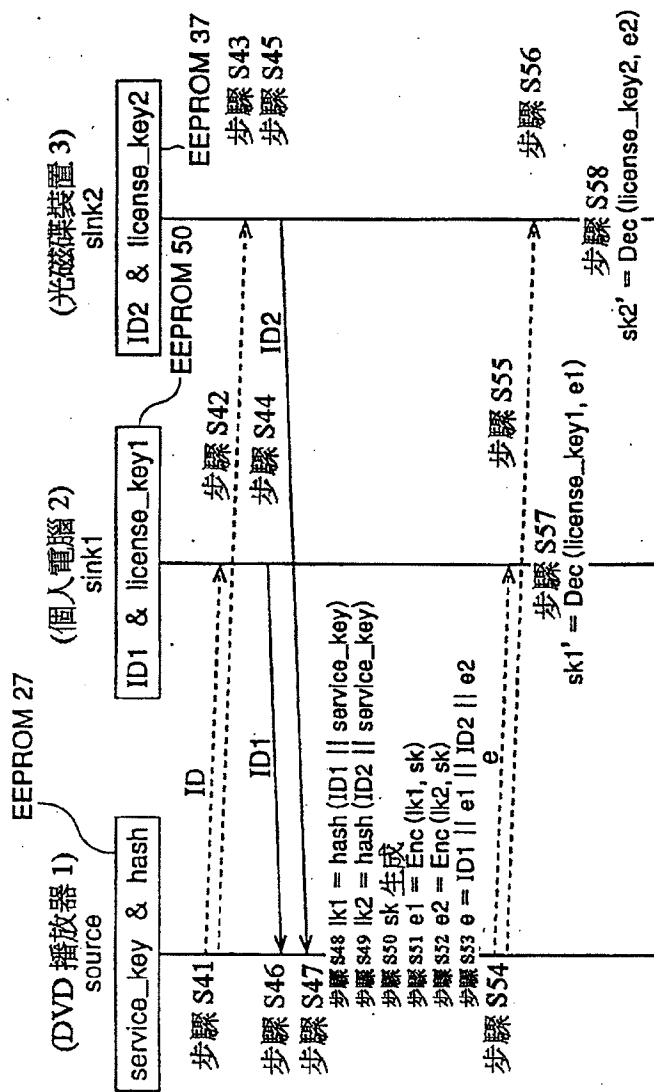
第 4 圖



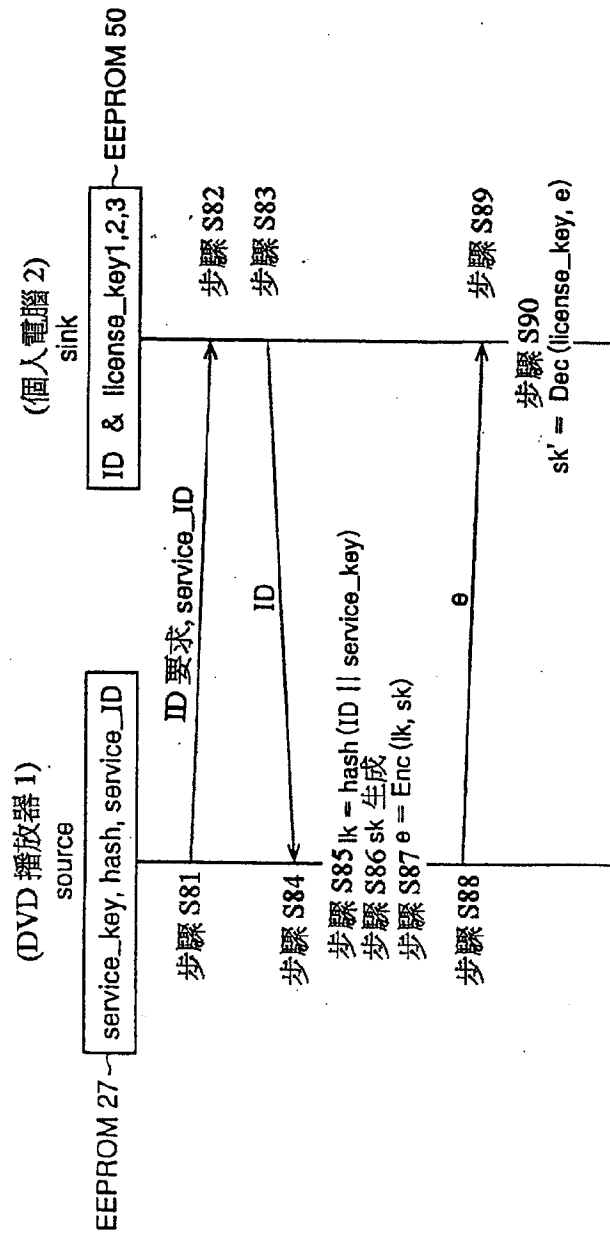
第 5 圖



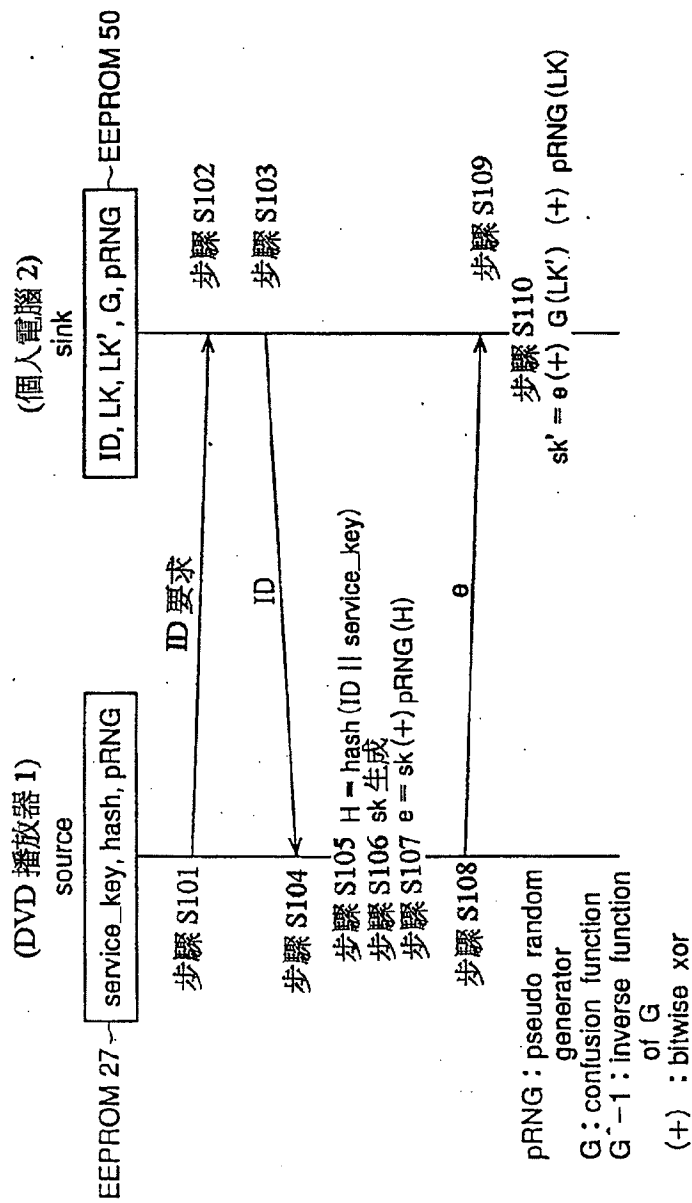
第 6 圖



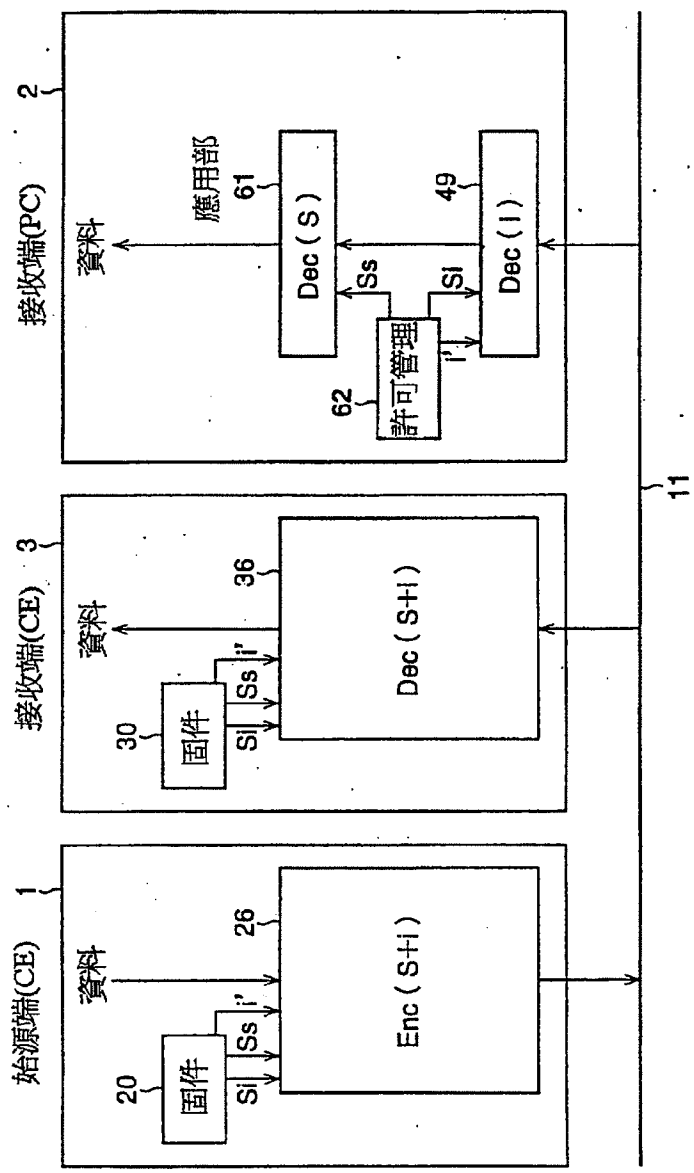
第 7 圖



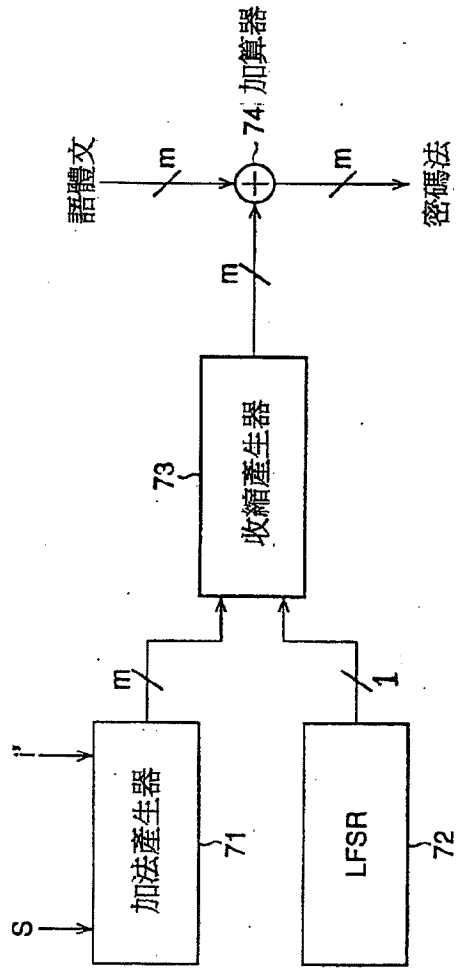
第 8 圖



第 9 圖

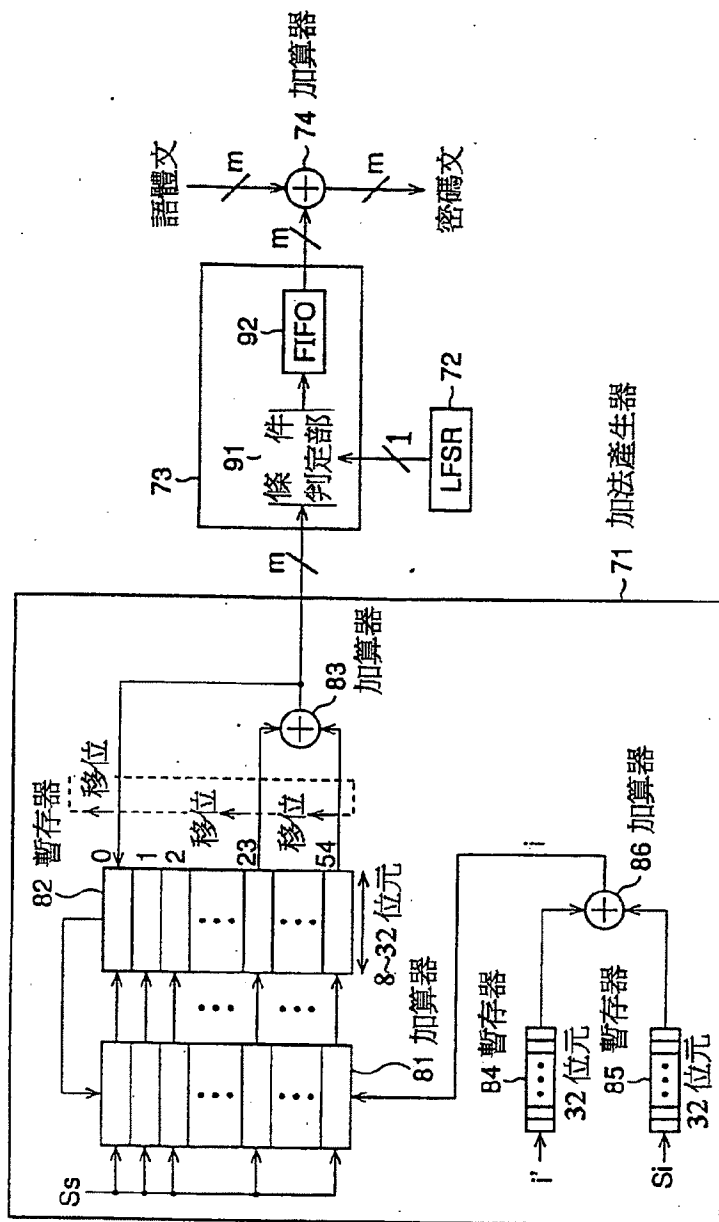


第10圖



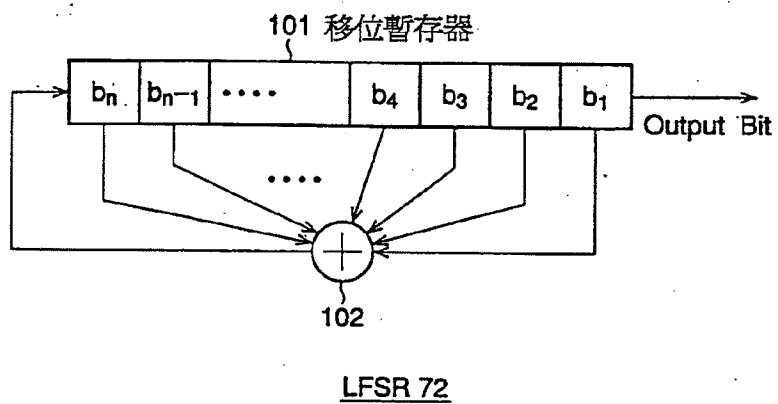
1394I/F 26
(始源端(CE))

第11圖

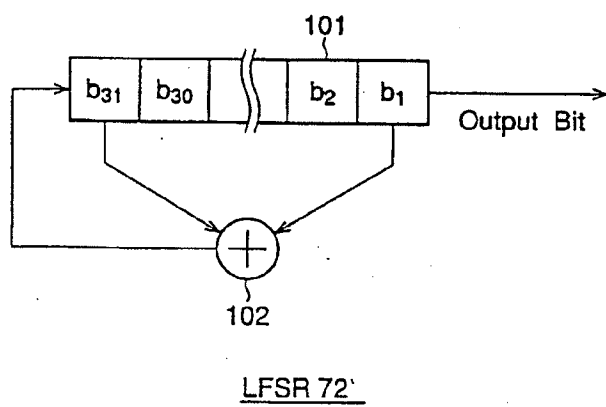


1394I/F 26
(接收端(CE))

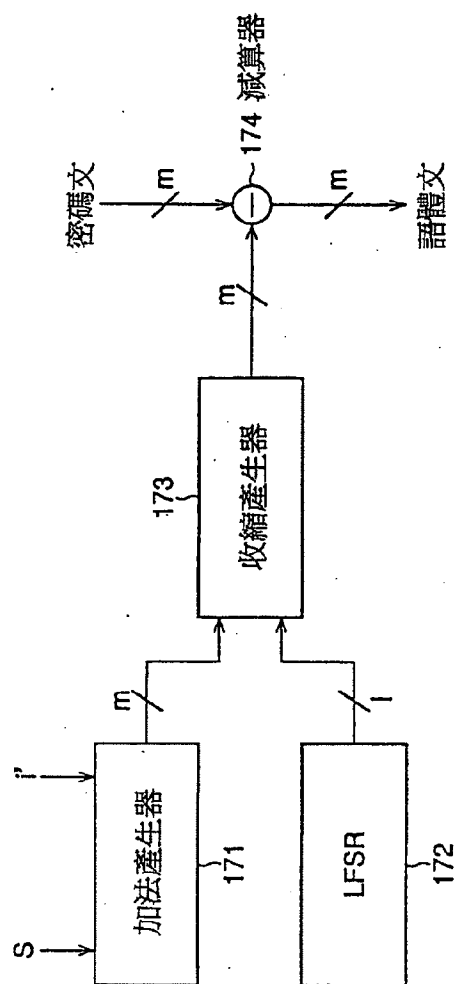
第12圖



第13圖

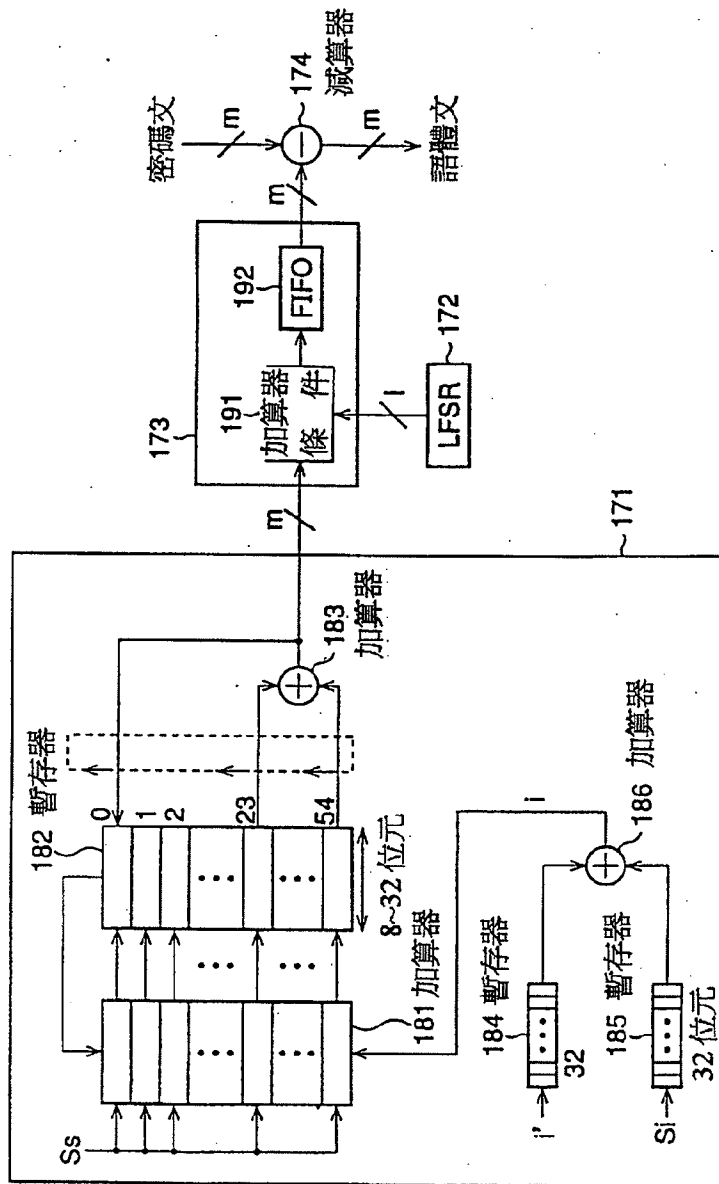


第14圖



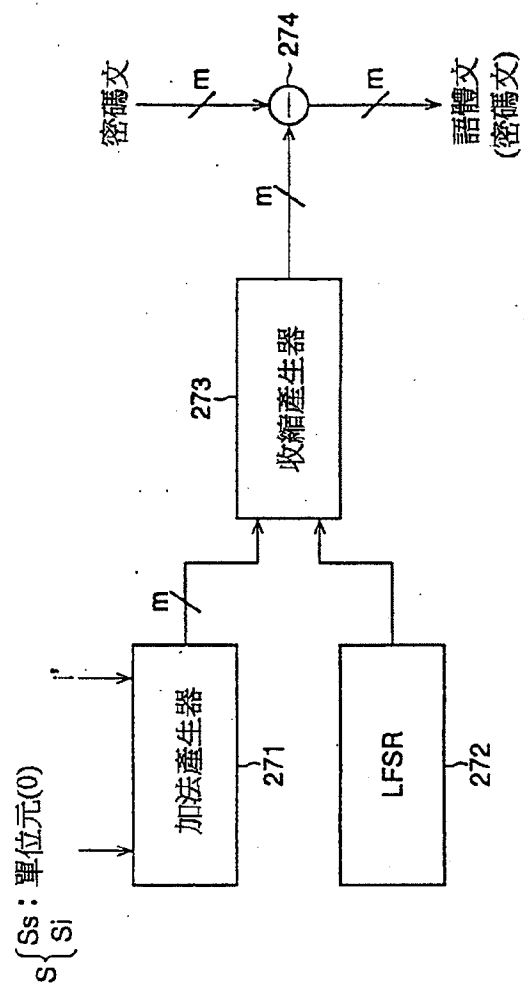
1394I/F 36
(接收端(CE))

第15圖



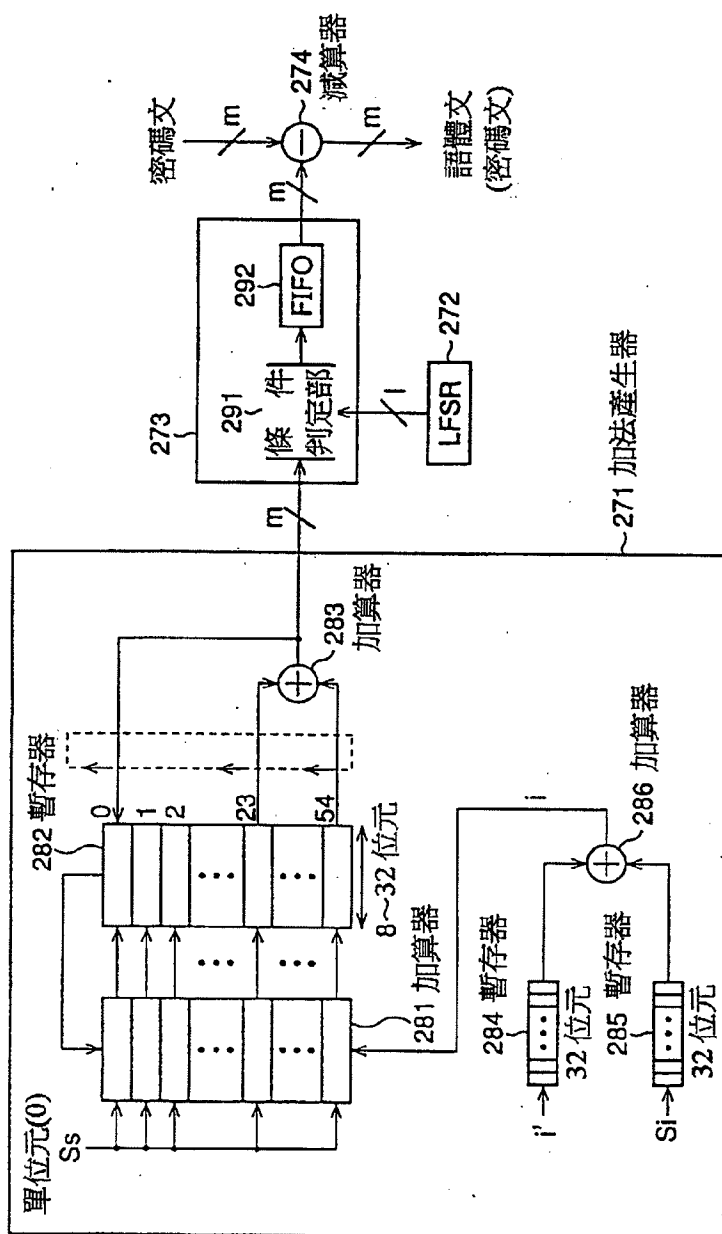
13941/F 36
(接收端(CE))

第16圖



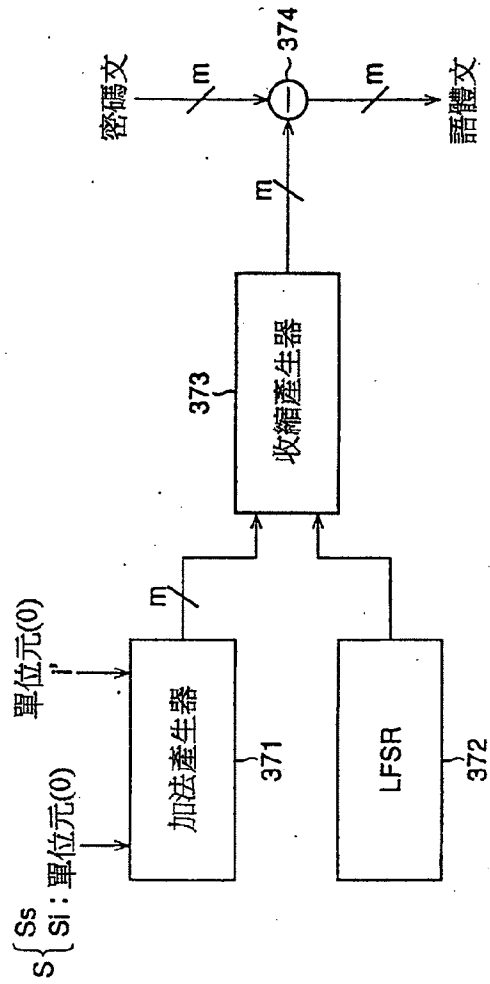
1394I/F49
(接收端(PC)的連結部分)

第17圖



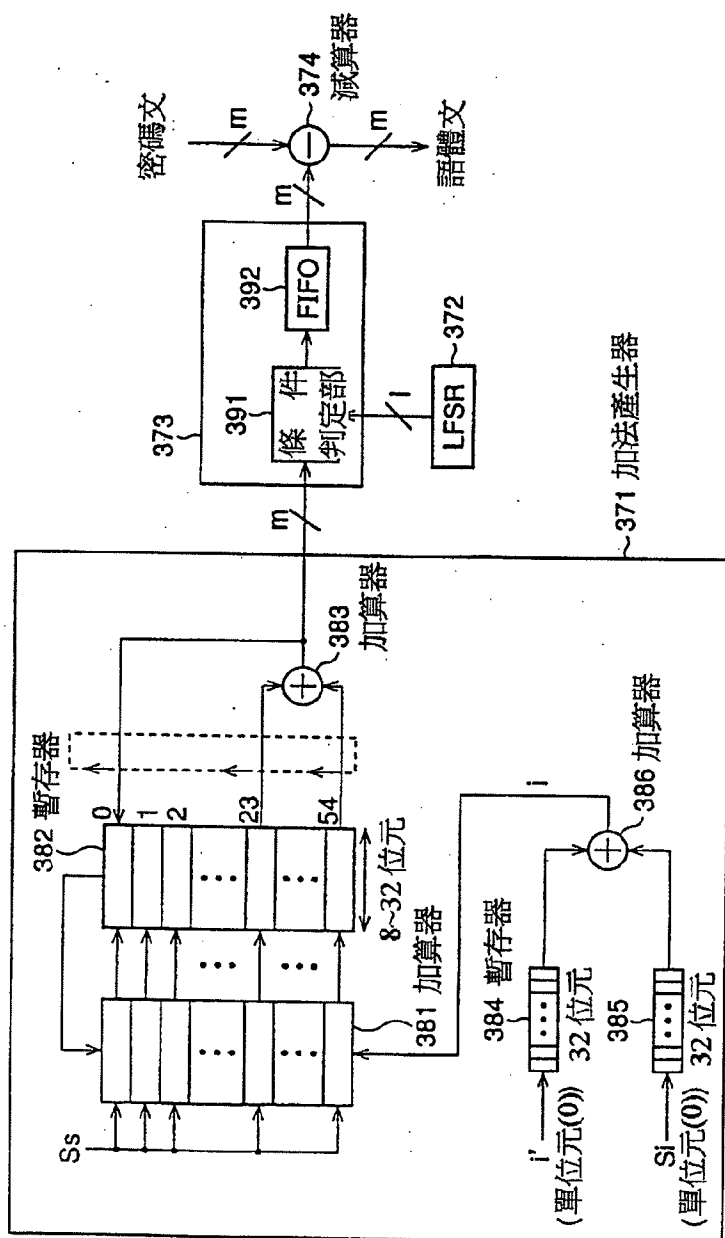
1394I/F49
(接收端(PC)的連結部分)

第18圖



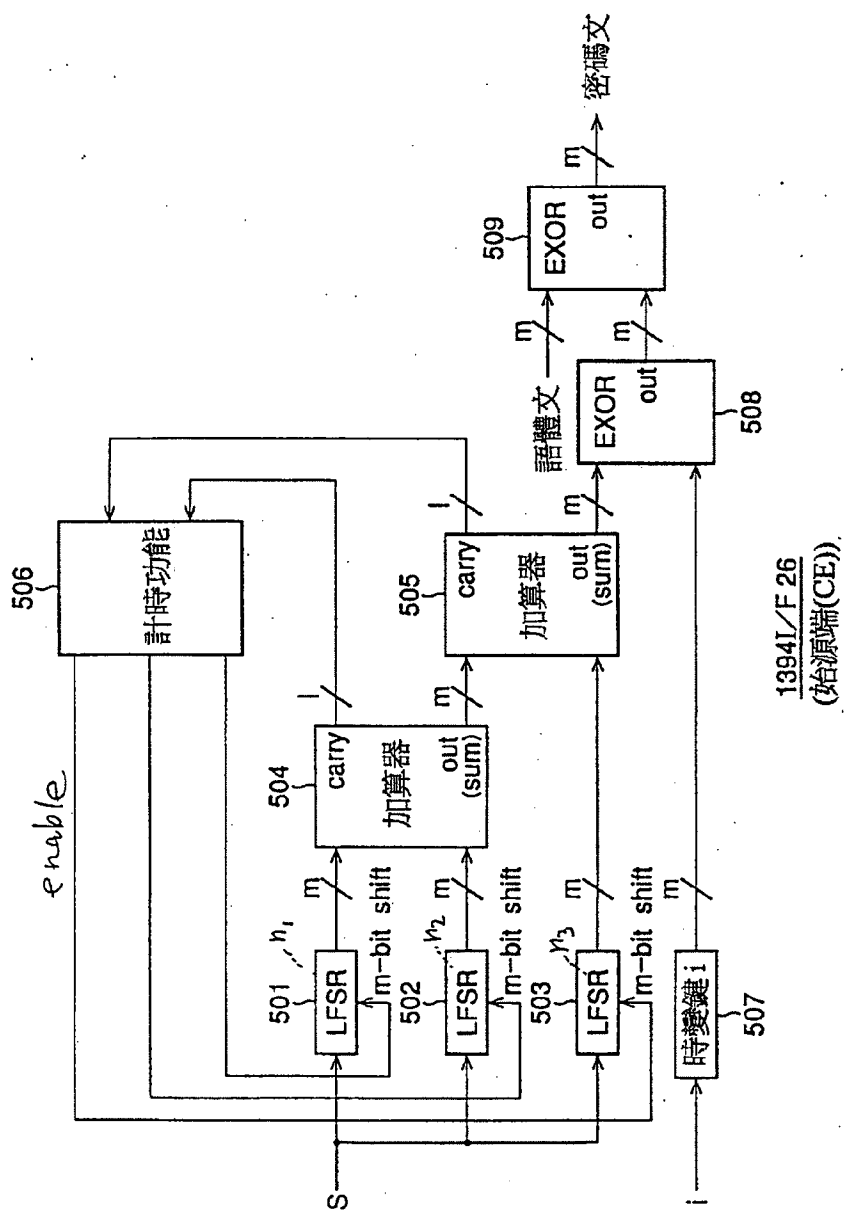
接收端(PC)的應用部 61

第19圖

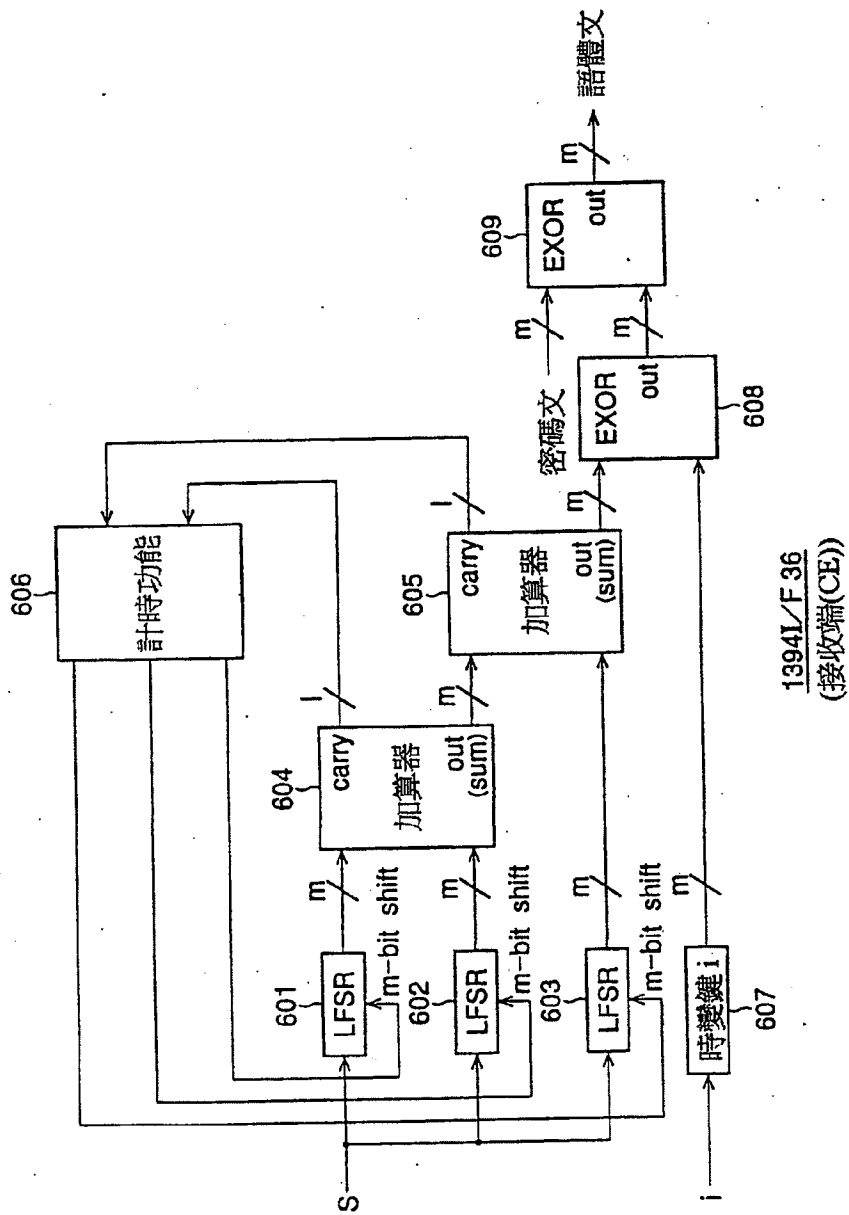


接收端(PC)的應用部 61

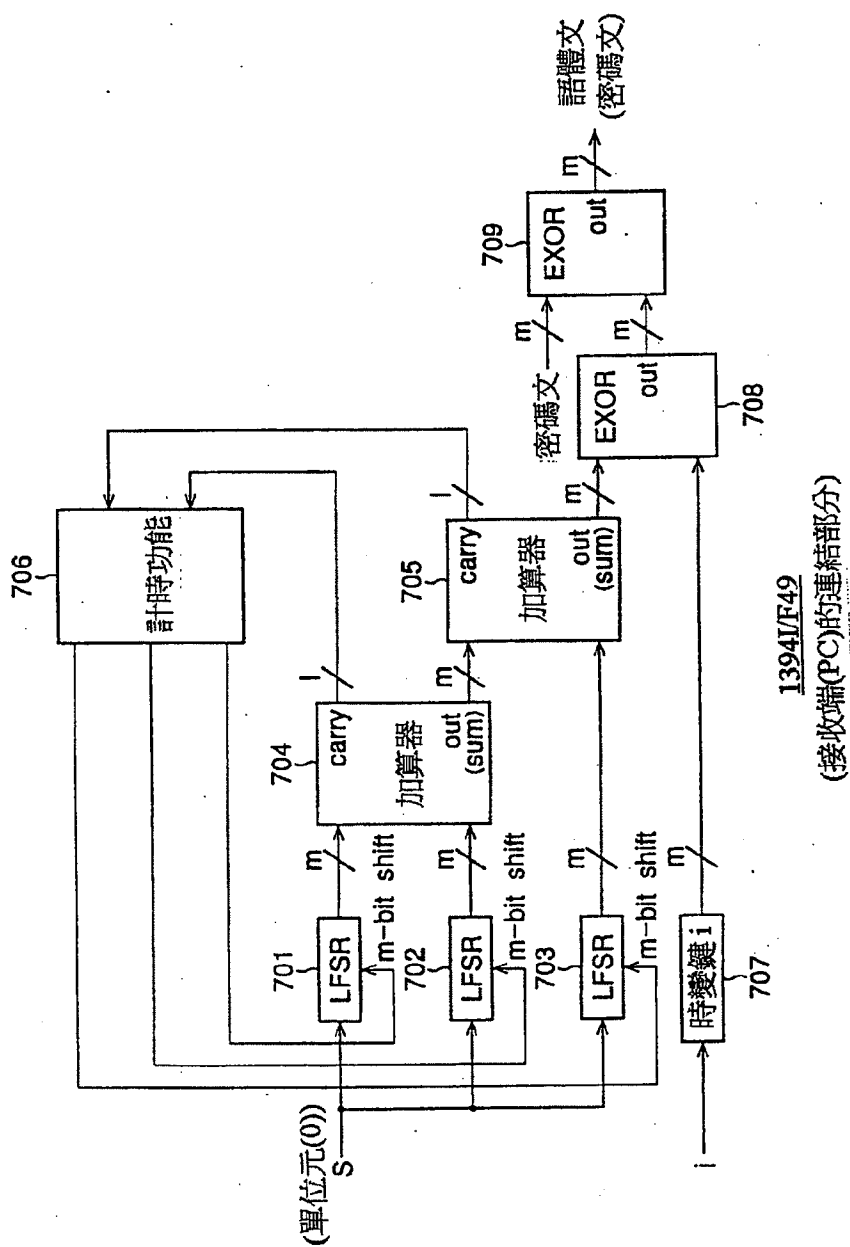
第20圖



第 21 圖



第22圖



第 23 圖

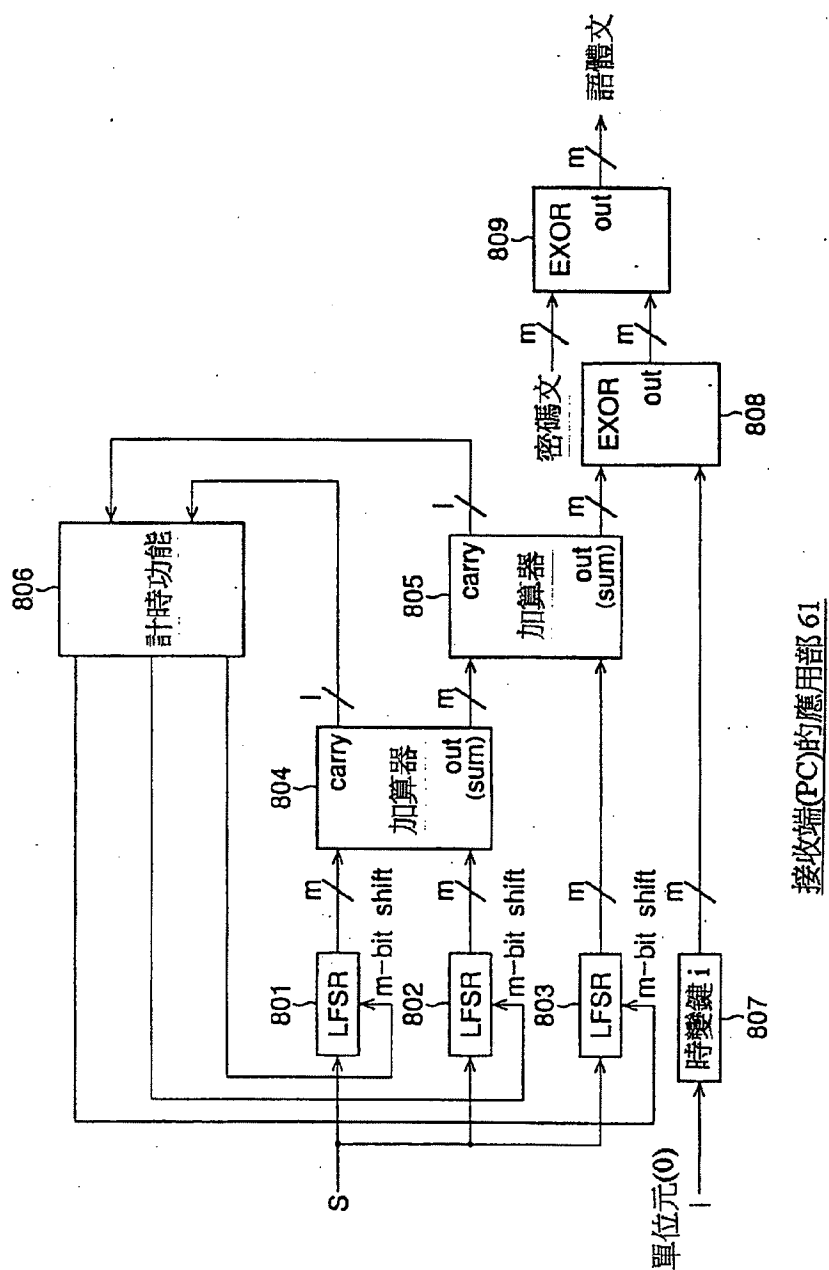


圖 24 第